EDIMAX
NETWORKING PEOPLE TOGETHER

EW-7438APn

User Manual

07-2013 / v1.0

CONTENTS

I. Product Information 4

I-1. Package Contents 4
I-2. System Requirements 4
I-3. Hardware Overview 4
I-4. LED Status 5
I-5. Safety Information 6

II. Installation 7

II-1. iQ Setup: Change Wi-Fi SSID & Password 10
II-2. Reset 15
II-3. Wi-Fi Protected Setup (WPS) 16

III. Browser Based Configuration Interface 17

III-1. Home 21
III-2. Status 22
III-3. Basic Settings 24
III-3-1. AP 25
III-3-2. AP Bridge-Point to Point 27
III-3-3. AP Bridge-Point to Multi-Point 28
III-3-4. AP Bridge-WDS 29
III-4. WPS Settings 31
III-5. Wireless Advanced 33
III-5-1. Security 36
III-5-1-1. Disable 37
III-5-1-2. WEP 37
III-5-1-3. WPA Pre-Shared Key 38
III-5-1-4. WPA Radius 39
III-5-1-5. Enable 802.1x Authentication 40
III-5-2. MAC Filtering 41
III-6. System Utility 43
III-6-1. Time Setting 46
III-6-2. Power Saving 47
III-6-3. Scheduling Setting 48
III-7 Configuration Tool 50
III-7-1. Diagnosis 51
III-7-2. Firmware Upgrade 52
III-7-3. Reboot 53

IV. Appendix 54

IV-1. Configuring your IP address 54
IV-1-1. How to check that your computer uses a dynamic IP address 55
IV-1-1-1. Windows XP 55
IV-1-1-2. Windows Vista 57
IV-1-1-3. Windows 7 59
IV-1-1-4. Windows 8 62
IV-1-1-5. Mac OS 66
IV-1-2. How to modify the IP address of your computer 68
IV-1-2-1. Windows XP 68
IV-1-2-2. Windows Vista 70
IV-1-2-3. Windows 7 72
IV-1-2-4. Windows 8 76
IV-1-2-5. Mac 80
IV-1-3. How to Find Your Network Security Key 83
IV-1-3-1. Windows 7 & Vista 83
IV-1-3-2. Mac 85
IV-1-4. How to Find Your Router's IP Address 88
IV-1-4-1. Windows XP, Vista & 7 88
IV-1-4-2. Windows 8 90
IV-1-4-3. Mac 93
IV-1-4. Troubleshooting 95
IV-1-5. Glossary 97

I. Product Information

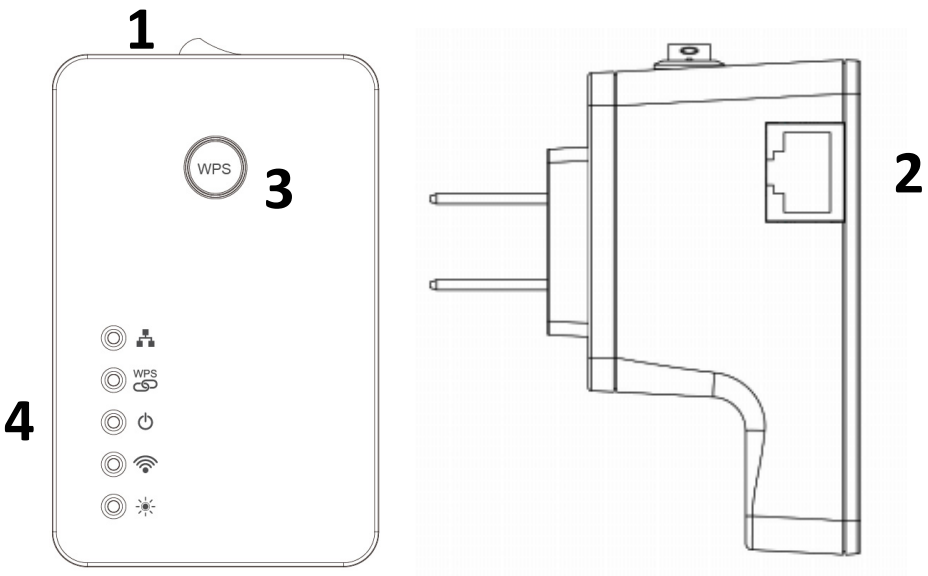
I-1. Package Contents

- EW-7438APn access point
- CD with multi-language QIG & user manual
- Quick installation guide
- RJ45 Ethernet cable
- Access key card

I-2. System Requirements

- Cable/DSL modem router
- Computer with 2.4GHz wireless adapter and web browser: Microsoft® Internet Explorer® 8.0 or above, Google Chrome®, Firefox® or Safari®

I-3. Hardware Overview



1. Power On/Off Switch

2. Ethernet Port

3. WPS/Reset Button

4. LEDs

I-4. LED Status

LED	Color	Status	Description
LAN	Green	On	LAN port connected.
		Flashing	LAN activity (transferring or receiving data).
		Off	LAN port not connected.
WPS	Green	On	WPS connection established (LED will remain on for 5 minutes).
		Flashing	WPS is active and waiting for a connection.
		Off	No WPS in progress.
Power	Green	On-	Access point is on.
		Off	Access point is off.
Wi-Fi	Green	Flashing	Wireless activity (transferring or receiving data).
		Off	No wireless activity.
Status	Orange	On	Access point is ready for use.
		Flashing	Access point is upgrading firmware or resetting to factory default status.
		Off	Access point is not ready for use.

I-5. Safety Information

In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.

1. The access point is designed for indoor use only; do not place the access point outdoors.

2. Do not place the access point in or near hot/humid places, such as a kitchen or bathroom.

3. Do not pull any connected cable with force; carefully disconnect it from the access point.

4. Handle the access point with care. Accidental damage will void the warranty of the access point.

5. The device contains small parts which are a danger to small children under 3 years old. Please keep the access point out of reach of children.

6. Do not place the access point on paper, cloth, or other flammable materials. The access point may become hot during use.

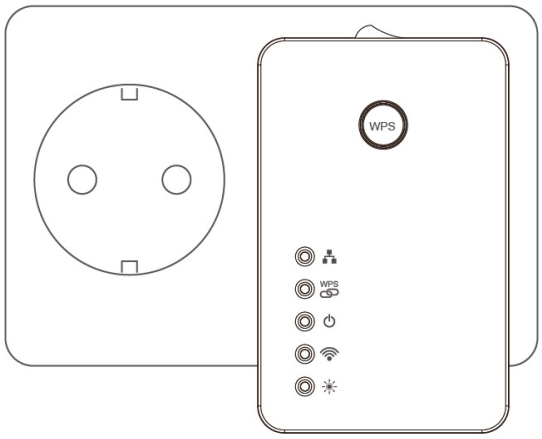
7. There are no user-serviceable parts inside the access point. If you experience problems with the access point, please contact your dealer of purchase and ask for help.

8. The access point is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.

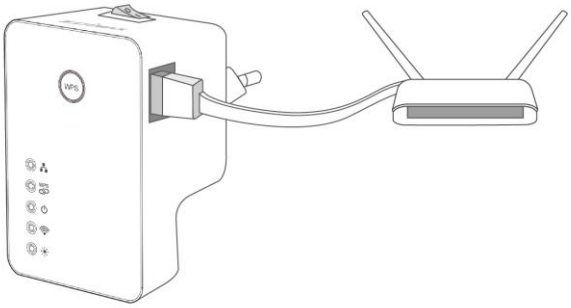
9. If you smell burning or see smoke coming from the access point or power adapter, then disconnect the access point and power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

II. Installation

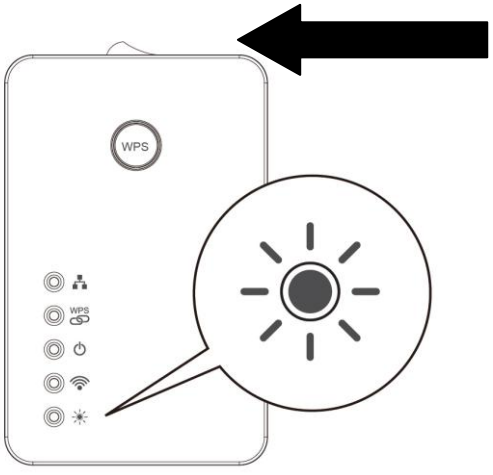
1. Plug the access point into a power socket.



2. Connect the access point to your existing router via Ethernet cable and ensure your router is turned on.



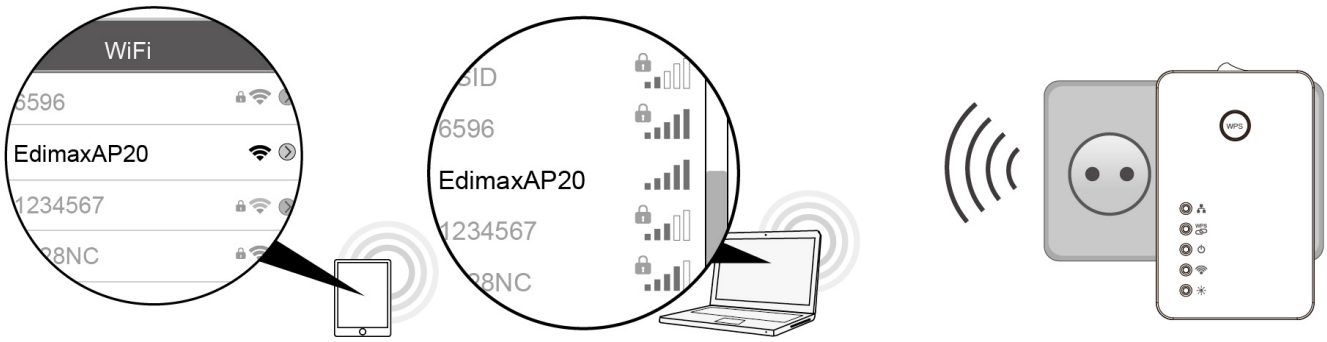
3. Switch the access point on using the on/off switch on the top of the device. The **green** power LED should display **on**. The access point may take a couple of minutes to boot up, and is ready when the **orange** status LED displays **on**.



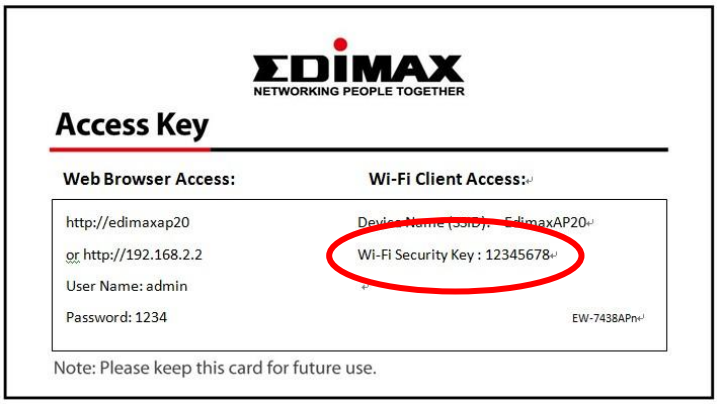
Switch power on

4. Use a Wi-Fi device (e.g. computer, tablet, smartphone) to search for a Wi-Fi network with the SSID "EdimaxAP**" and connect to it.

The last two characters of the SSID (**) will be unique numbers according to your access point e.g. EdimaxAP20. Your unique SSID is displayed on the product label along with the included access key card.



5. Enter the password to connect to the SSID. The password is eight characters and can be found on the label of the access point, and also on the access key card (Wi-Fi Security Key) included in the package contents.



6. Repeat steps **4** & **5** for any additional wireless devices you wish to connect to the Internet.

The access point is now ready for use. Open a web browser and you should be connected to the Internet.

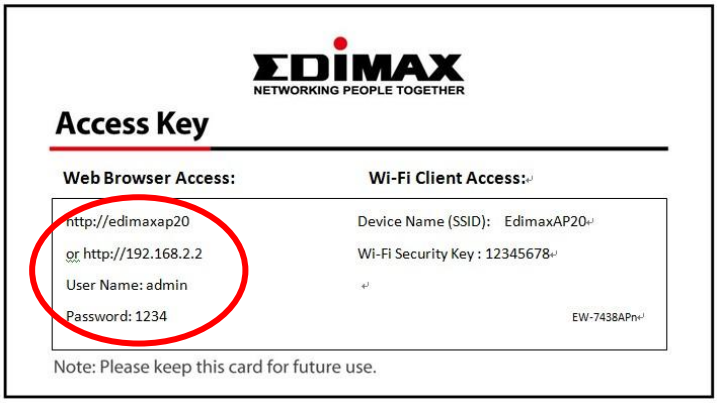
You can change the basic settings of the access point, such as the SSID & password, and guest SSID & password, using

*iQ Setup (see **II-1. iQ Setup: Changing Wi-Fi SSID & Password**).*

*For more advanced configurations, you can use the browser based configuration interface (refer **III. Browser Based Configuration Interface**).*

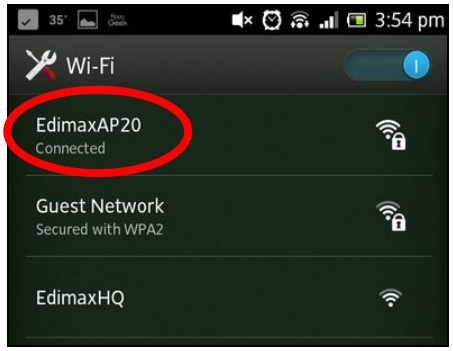
II-1. iQ Setup: Change Wi-Fi SSID & Password

Please check the access key card included in the package contents for your access point's unique SSID and URL.

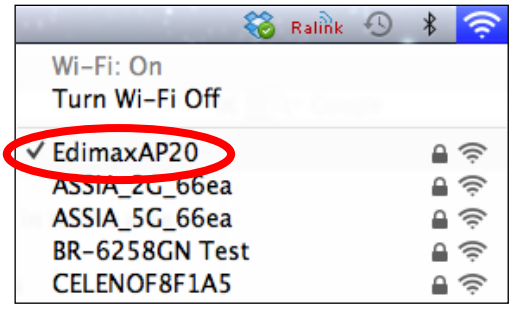


1. Ensure your Wi-Fi device (e.g. computer, tablet or smartphone) is connected to the access point's SSID "EdimaxAP**".

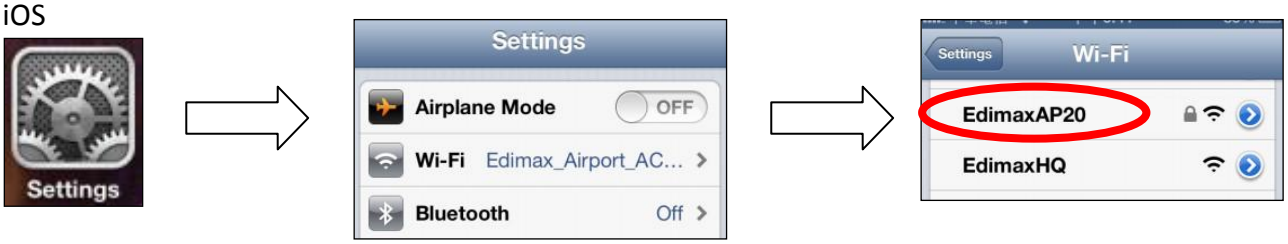
Android



Mac

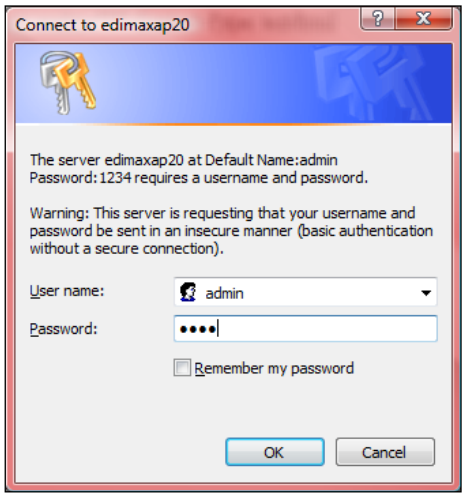


iOS

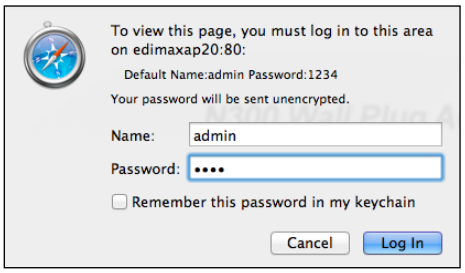


2. Go to your access point's unique URL *http://EdimaxAP**** in a web browser. Enter the username "admin" and password "1234".

Windows


Connect to edimaxap20
The server edimaxap20 at Default Name:admin Password:1234 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

Mac



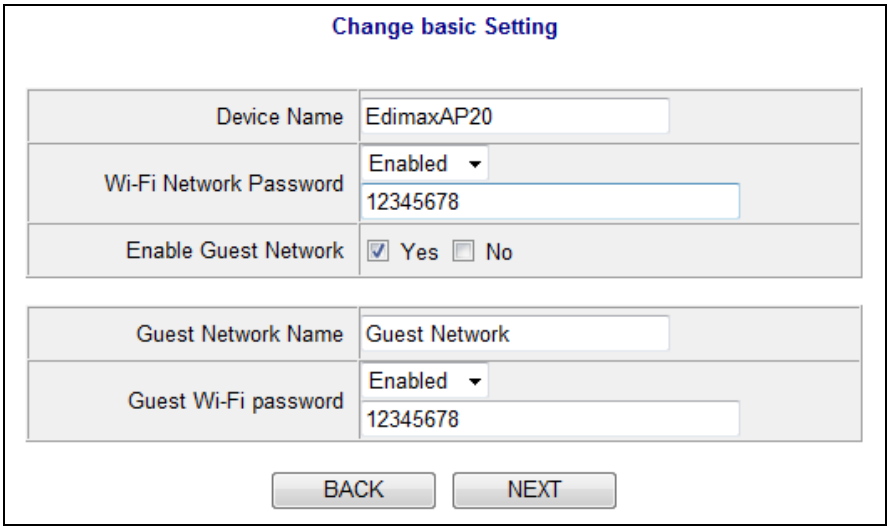
Your computer must be set to use a dynamic IP address for first time access to *http://EdimaxAP***. ***Static IP users can use the access point's default IP address*** *http://192.168.2.2* ***instead. For more information please refer to*** ***Appendix V-1. Configuring your IP Address*** **.**

3. Select "iQ Setup" to continue.

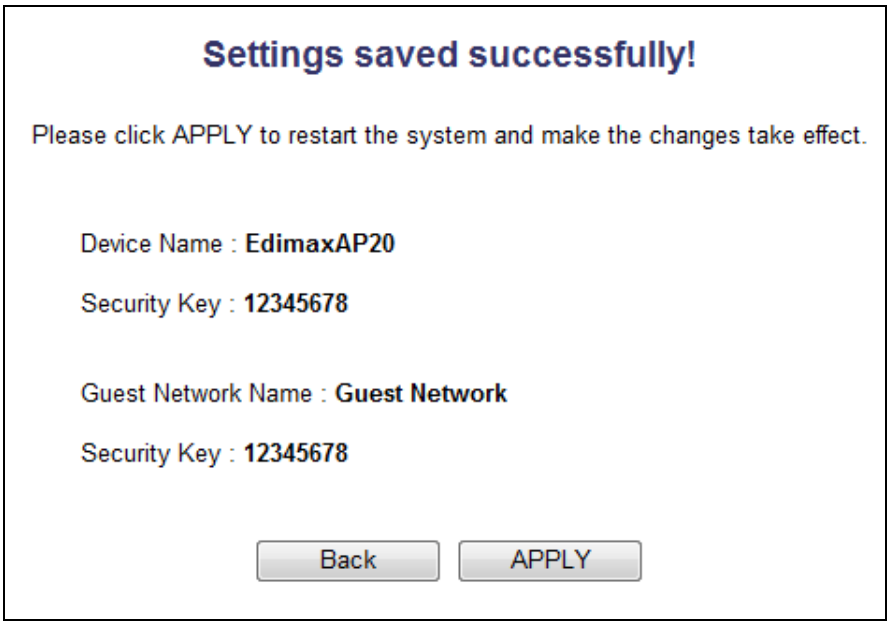
You can change the language using the drop down menu in the top right corner. For "Advanced" configurations please refer to III. Browser Based Configuration Interface.

4. The access point's basic settings will be displayed. Change the "Device/Guest Network Name" (SSID) or "Wi-Fi Network/Guest Wi-Fi Password" according to your preference." Click "Next" when you are ready to continue.

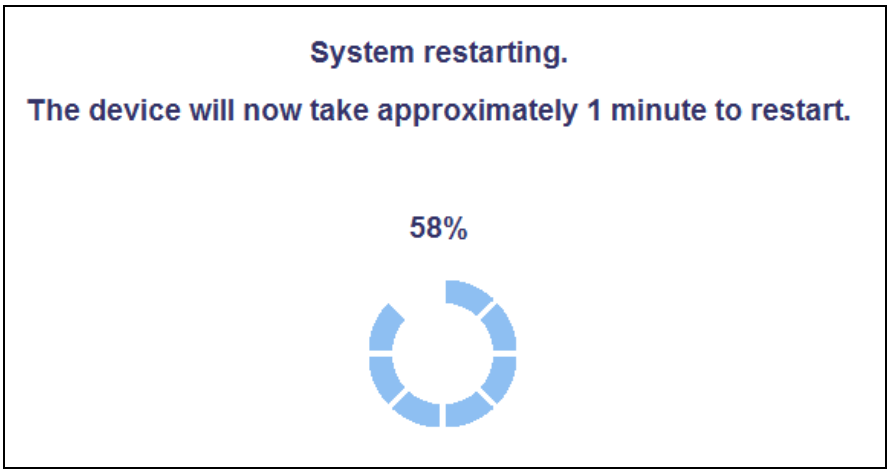
iQ Setup allows you to quickly configure an additional guest Wi-Fi network. To enable this feature check "Yes" for "Enable Guest Network". Additional SSIDs (up to four) can be configured using the browser based configuration interface.



5. A summary of your basic settings will be displayed. Please double check everything is correct and click "APPLY" to continue. Click "Back" if you wish to go back to the previous page.

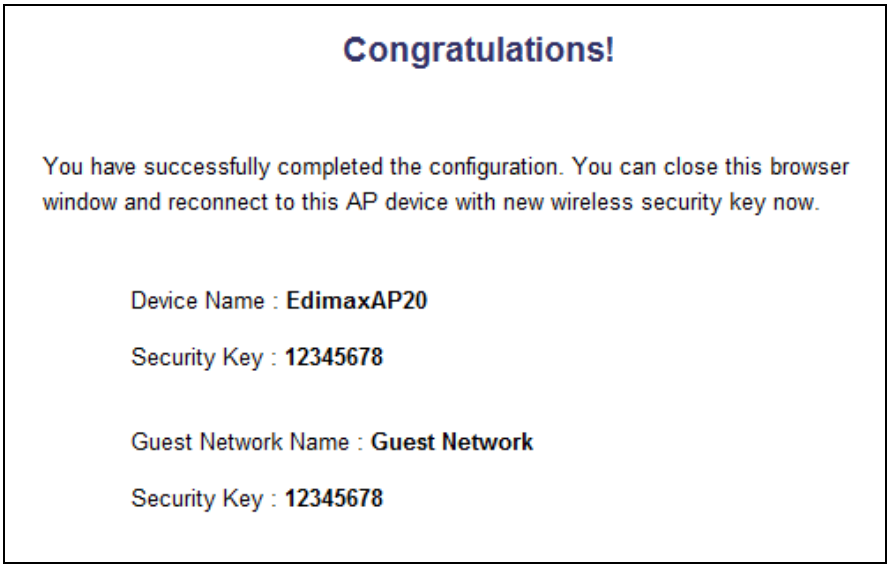

Settings saved successfully!
Please click APPLY to restart the system and make the changes take effect.
Device Name : EdimaxAP20
Security Key : 12345678
Guest Network Name : Guest Network
Security Key : 12345678
Back
APPLY

6. Please wait while the access point restarts.



7. You will see the following "Congratulations" screen to indicate that iQ Setup is complete, along with a summary of the access point's new settings.

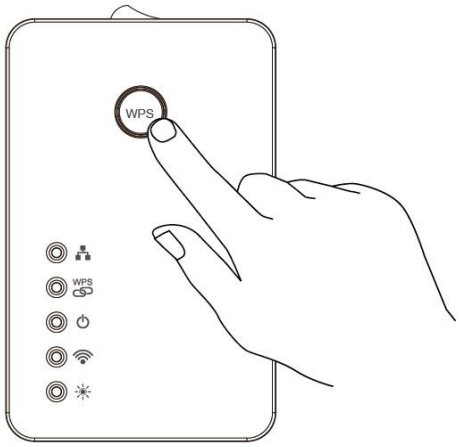
If you changed the access point's SSID, you will need to reconnect to the new SSID.


Congratulations!
You have successfully completed the configuration. You can close this browser window and reconnect to this AP device with new wireless security key now.
Device Name : EdimaxAP20
Security Key : 12345678
Guest Network Name : Guest Network
Security Key : 12345678

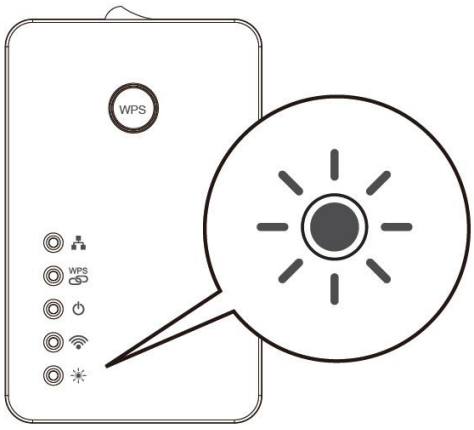
II-2. Reset

If you experience problems with your access point, you can reset the device back to its factory settings. This resets **all** settings back to default.

1. Press and hold the WPS/Reset button on the front of the access point for at least 10 seconds. Release the button when the **orange** status LED is **flashing**.



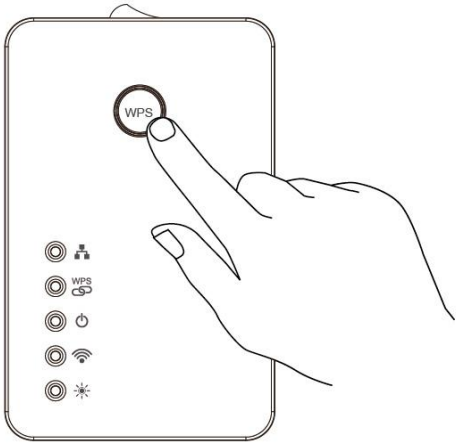
2. Wait for the access point to restart. The access point is ready for setup when the **orange** status LED displays **on**.



II-3. Wi-Fi Protected Setup (WPS)

After you have set up the access point as explained in **II. Installation** you can use the WPS button to establish a connection between the access point and a WPS-compatible wireless device/client.

1. Press and hold the WPS/Reset button on the front of the access point for 2 seconds. Release the button when the **green** WPS LED is **flashing**.



2. Within two minutes, activate WPS on your WPS-compatible wireless device. Please check the documentation for your wireless device for information regarding its WPS function.

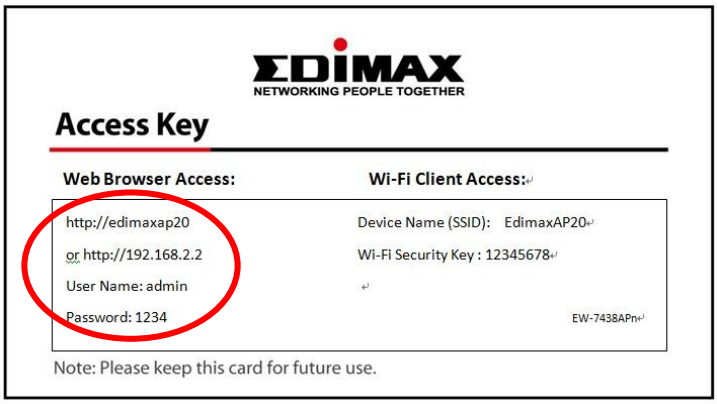
3. The devices will establish a connection. The access point's **green** WPS LED will display **on** for 5 minutes to indicate a successful connection.

III. Browser Based Configuration Interface

After you have setup the access point as detailed in **II. Installation**, you can use the browser-based configuration interface to configure advanced settings.

Mac users can also use the "Bonjour" function of Safari to access the browser based configuration interface.

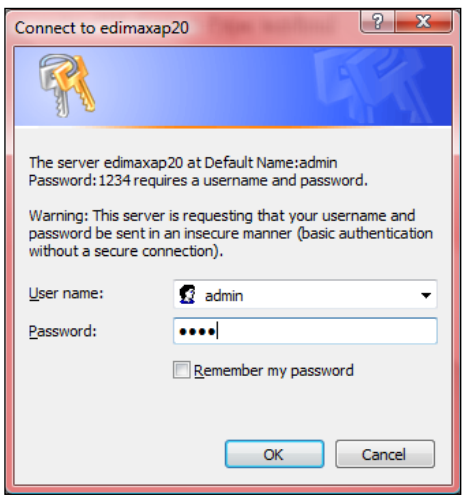
Please check the access key card included in the package contents for your access point's unique SSID and URL.



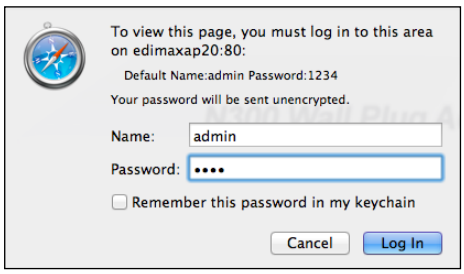
1. Ensure your Wi-Fi device (e.g. computer, tablet or smartphone) is connected to the access point's SSID "EdimaxAP**".

2. Go to your access point's unique URL *http://EdimaxAP*** in a web browser. Enter the username "admin" and password "1234".

Windows


Connect to edimaxap20
The server edimaxap20 at Default Name:admin Password:1234 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

Mac

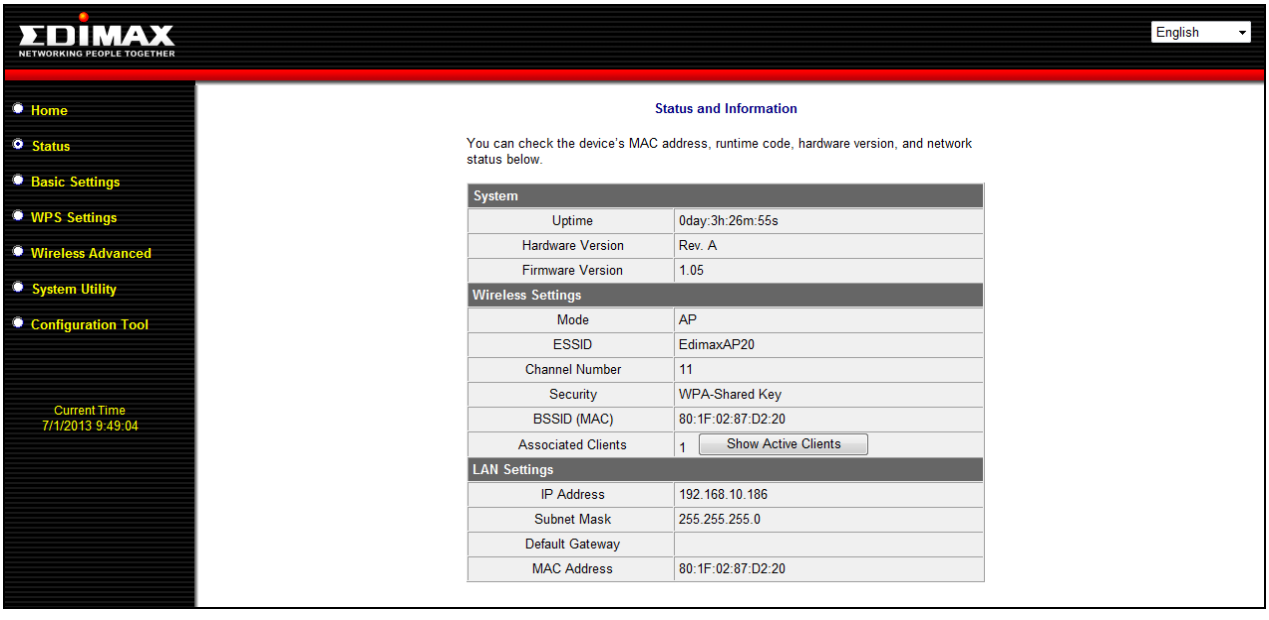


Your computer must be set to use a dynamic IP address for first time access to *http://EdimaxAP***. ***Static IP users can use the access point's default IP address*** *http://192.168.2.2* ***instead. For more information please refer to*** ***Appendix V-1. Configuring your IP Address*** **.**

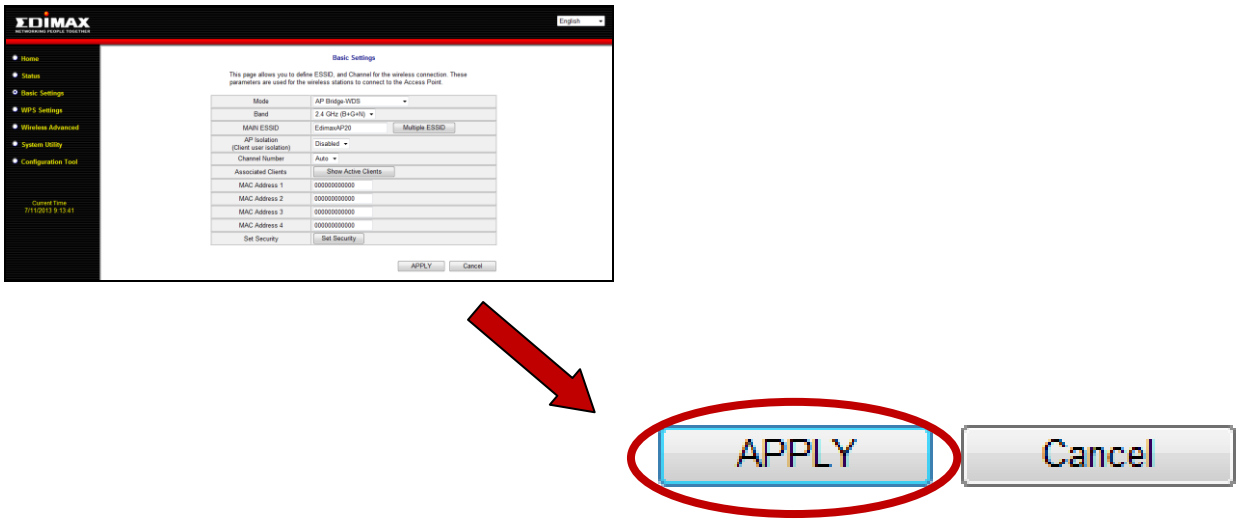
3. Select "Advanced" to go to the browser based configuration interface.

4. You will arrive at the "Status" screen shown below. Use the menu down the left side to navigate.

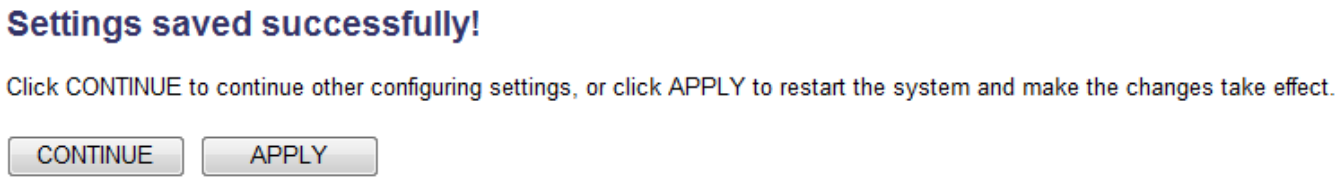
You can change the language using the drop-down menu in the top right corner.



5. After you make any changes to the access point's settings, please click "APPLY".



Then, select "CONTINUE" to save changes but not apply them yet or select "APPLY" to restart the access point and bring the changes into effect.

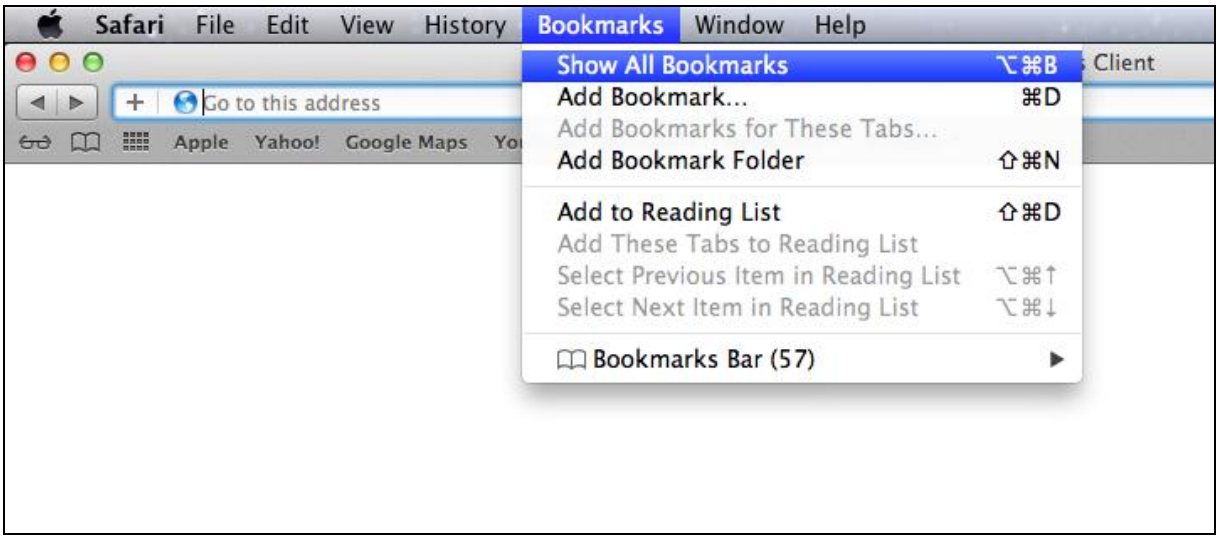

Settings saved successfully!
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.
CONTINUE
APPLY

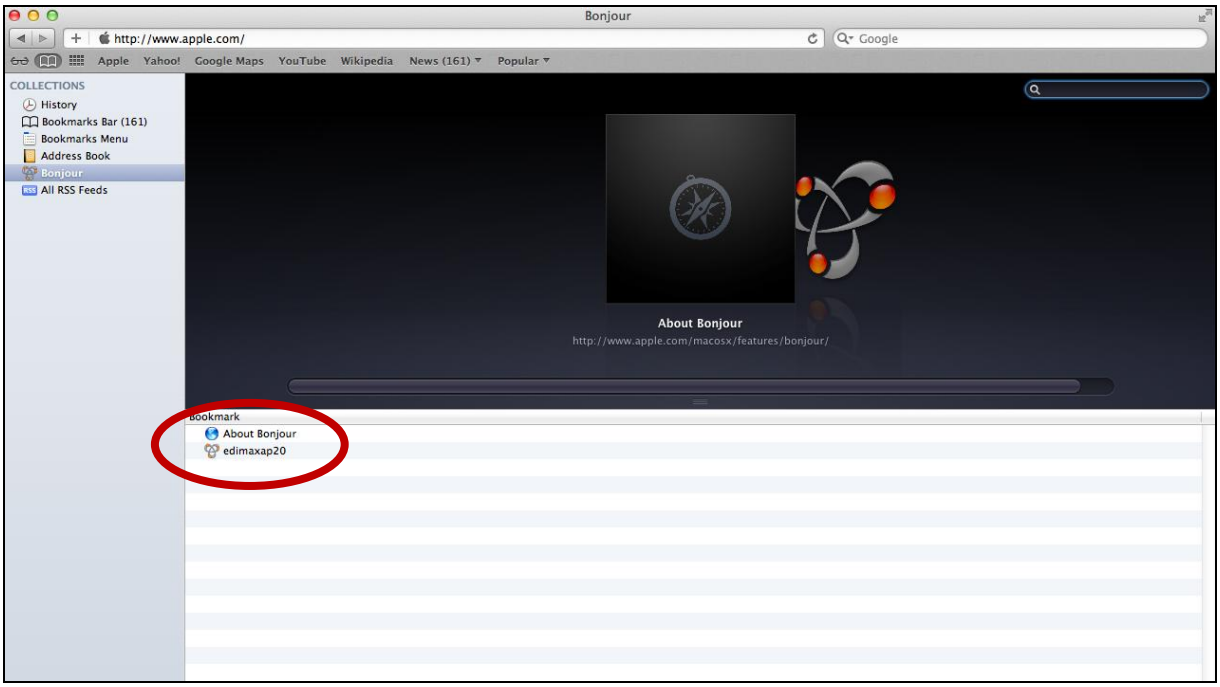
The access point needs to restart in order to apply and bring any changes into effect. Use the "CONTINUE" button to make several changes and apply them all together in one restart.

Mac: Bonjour

Open **Safari** web browser and open the “Bookmarks” menu across the top of the screen, and select “Show All Bookmarks”. Or you can click on the bookmarks icon under the URL bar.

Then, select “Bonjour” from the menu in the left panel. Finally, click on “edimaxAP**” in the lower panel on the right side.





III-1. Home

From the “Home” page you can choose to run iQ Setup again to quickly configure the access point’s basic settings (see **II-1. iQ Setup**), or select “Advanced” go to the browser based configuration interface to configure the access point’s advanced settings.

Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

III-2. Status

The “Status” page displays basic system information about the access point.

Status and Information

You can check the device’s MAC address, runtime code, hardware version, and network status below.

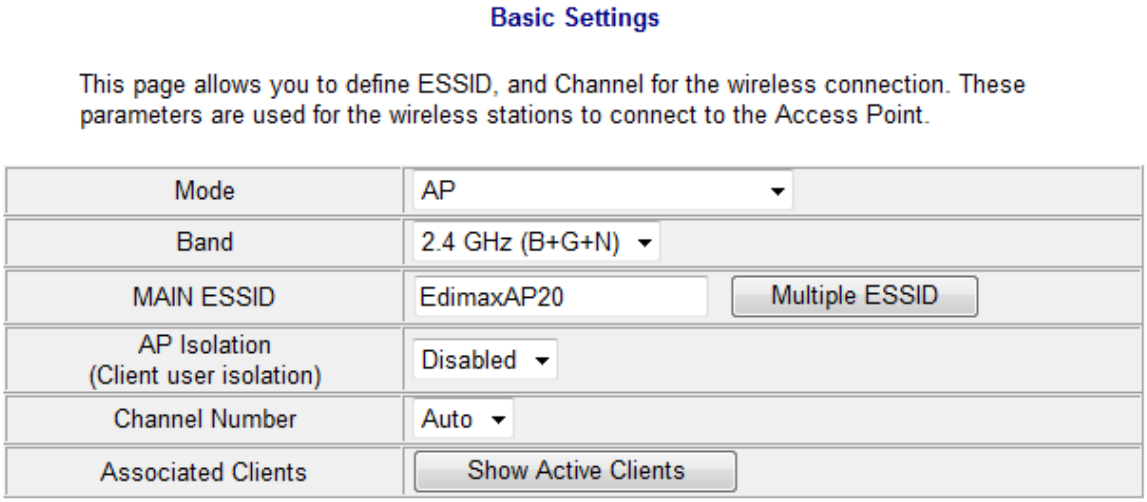
System	
Uptime	0day:4h:36m:13s
Hardware Version	Rev. A
Firmware Version	1.05
Wireless Settings	
Mode	AP
ESSID	EdimaxAP20
Channel Number	11
Security	WPA-Shared Key
BSSID (MAC)	80:1F:02:87:D2:20
Associated Clients	1 Show Active Clients
LAN Settings	
IP Address	192.168.10.186
Subnet Mask	255.255.255.0
Default Gateway	
MAC Address	80:1F:02:87:D2:20

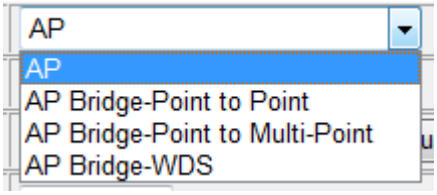
Uptime	Displays the total time since the device was turned on.
Hardware Version	Displays the hardware version.
Firmware Version	Displays the firmware version.
Mode	Displays the operating mode.
ESSID	Displays the access point’s ESSID, sometimes also known as SSID. The ESSID/SSID is the name used to identify a wireless network.
Channel Number	Displays the current wireless channel number.
Security	Displays the current wireless security setting.
BSSID (MAC)	Displays the device’s BSSID. The BSSID identifies this access point in the network, and is the same as the device’s MAC address.

Associated Clients	Displays the number of clients connected to the access point. Click “Show Active Clients” to display a new window showing information about wireless clients.
IP Address	Displays the IP address of this device.
Subnet Mask	Displays the subnet mask of the IP address.
Default Gateway	Displays the IP address of the default gateway.
MAC address	Displays the device’s MAC address. The MAC address is a unique, fixed ID for this device, it cannot be modified.

III-3. Basic Settings

The access point has four different operating modes. “Basic Settings” allows you to change the mode and configure the settings for each mode.



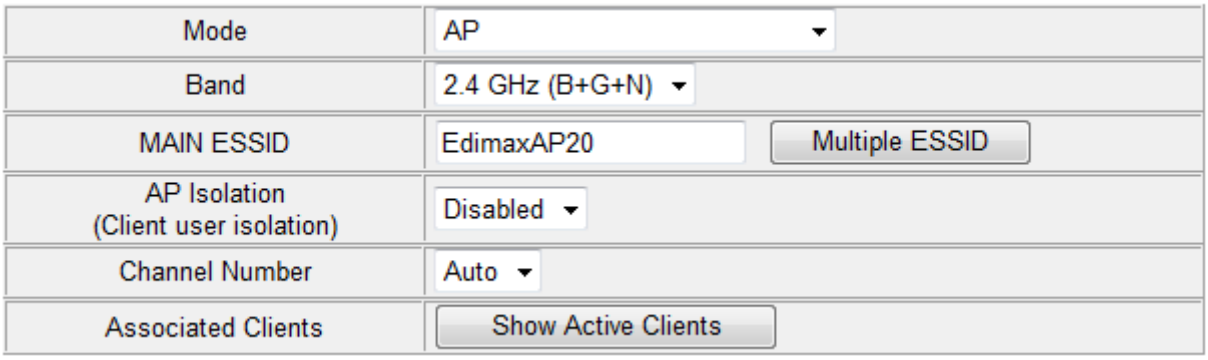


AP	The device acts as a wireless “access point” to a wired Ethernet network. Wireless clients can connect to this device and exchange data with devices connected to the wired network.
AP Bridge-Point to Point	Establishes a wireless connection with another wireless access point using the same mode, and links any wired networks connected to these two wireless access points together. Only one access point can be connected in this mode.
AP Bridge-Point to Multi-Point	Establishes a wireless connection with other wireless access points using the same mode, and links any wired networks connected to these wireless access points together. Up to four access points can be connected in this

	mode.
AP Bridge-WDS	This mode is similar to “AP Bridge to Multi-Point”, but the device is not in bridge-dedicated mode, and will be able to accept wireless clients.

III-3-1. AP

In access point (AP) mode the device acts as a wireless access point to a wired Ethernet network for IEEE 802.11b/g/n wireless devices.

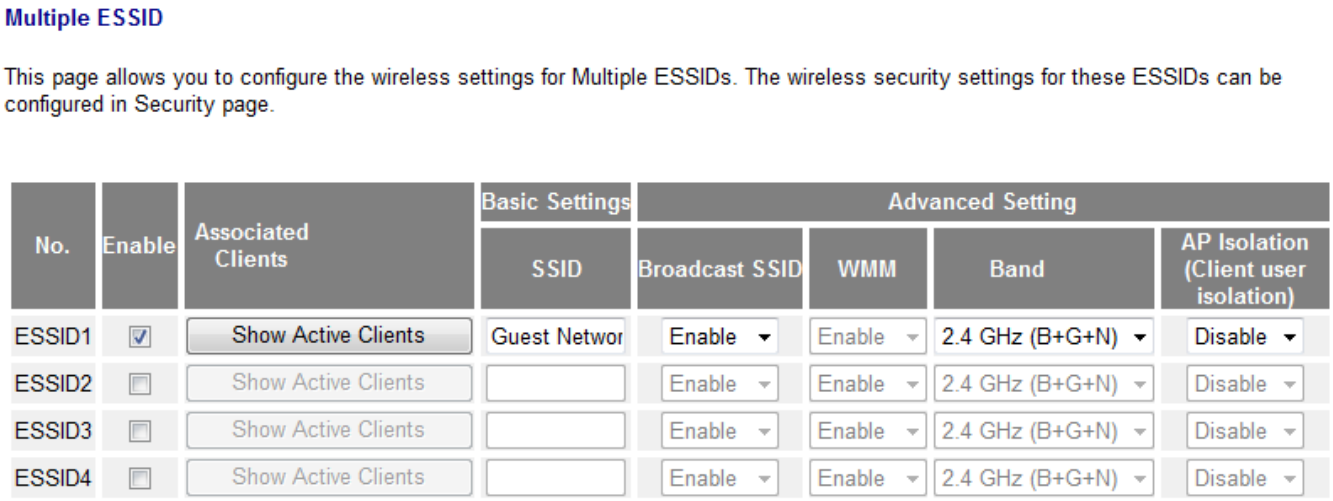


Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only wireless clients of the same band(s) as you select will be able to connect.
MAIN ESSID	Specify an ESSID (the name used to identify the access point) of up to up to 32 alphanumerical characters. **Please note that the ESSID is case sensitive.**
Multiple ESSID	Click “Multiple ESSID” to open a new window and assign up to four ESSIDs to this access point. Please see the following page for more details.
AP Isolation	When “Enabled”, wireless clients will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the MAIN ESSID only.
Channel Number	Select a channel number for the access point. Where possible, select a channel number

	which is not already in use by another access point/router.
Associated Clients	Click “Show Active Clients” to display a new window showing information about wireless clients.

Multiple ESSID

This page allows you to configure the wireless settings for multiple ESSID’s.



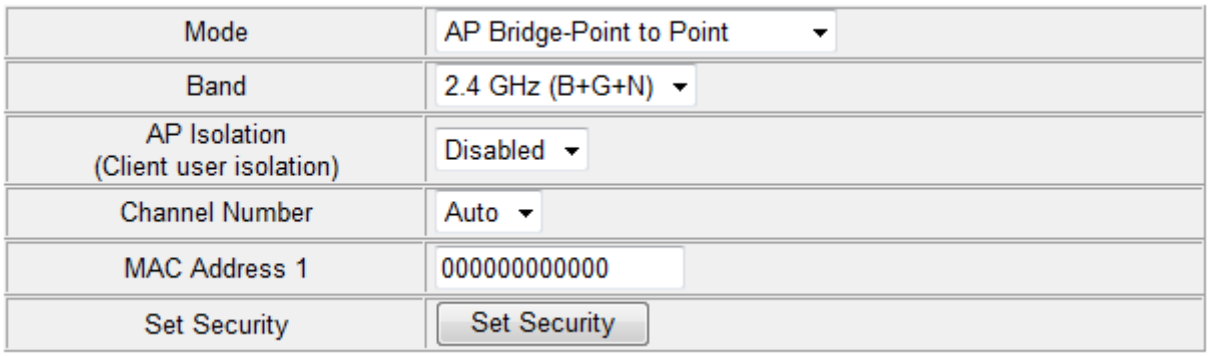
No.	Identification number of each additional ESSID.
Enable	Check the box to enable or disable an ESSID.
SSID	Enter the SSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. **Please note that the ESSID is case sensitive.**
Broadcast SSID	Set if the access point will broadcast its own ESSID. To hide the ESSID of your access point select “Disable” (only users who know the ESSID of your access point will be able to connect).
WMM	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When WMM is enabled, the access point will prioritize different kinds of data and give higher priority to applications which require

	instant responses. This improves the performance of such network applications.
Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only wireless clients of the same band(s) as you select will be able to connect.
AP Isolation	When “Enabled”, wireless clients will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the MAIN ESSID only.

III-3-2. AP Bridge-Point to Point

In AP bridge-point to point mode, the access point connects to another wireless access point in the same mode, and all connected Ethernet clients of both devices are connected together. This allows two physically isolated networks to communicate with each other.

When using this mode, the access point will not accept regular clients.



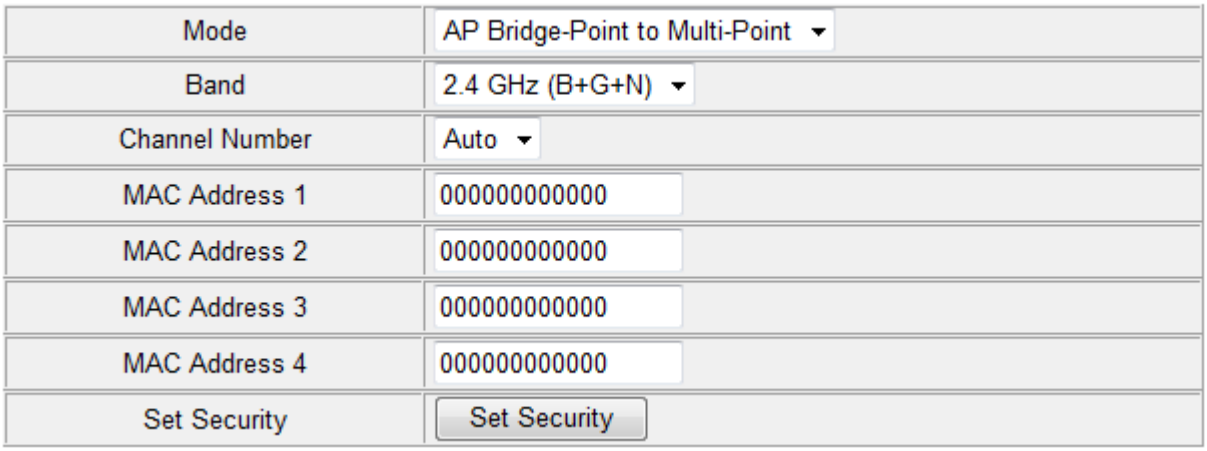
Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only access points of the same band or bands as you select will be able to connect.
AP Isolation	When “Enabled”, wireless clients will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the MAIN ESSID only.
Channel Number	Select a channel number for the access point.

	The channel number must be the same as the other access point you wish to connect to.
MAC address 1	Enter MAC address of the wireless access point you wish to connect to.
Set Security	Click “Set Security” to select an encryption mode for this wireless link. A new window with security options will appear. See **III-5-1. Security.**

III-3-3. AP Bridge-Point to Multi-Point

In AP bridge-point to multi-point mode the access point can connect to up to four other wireless access points also using the same mode, and all connected Ethernet clients of all access points will be connected together. This allows several physically isolated networks to communicate with each other.

When using this mode, the access point will not accept regular clients.



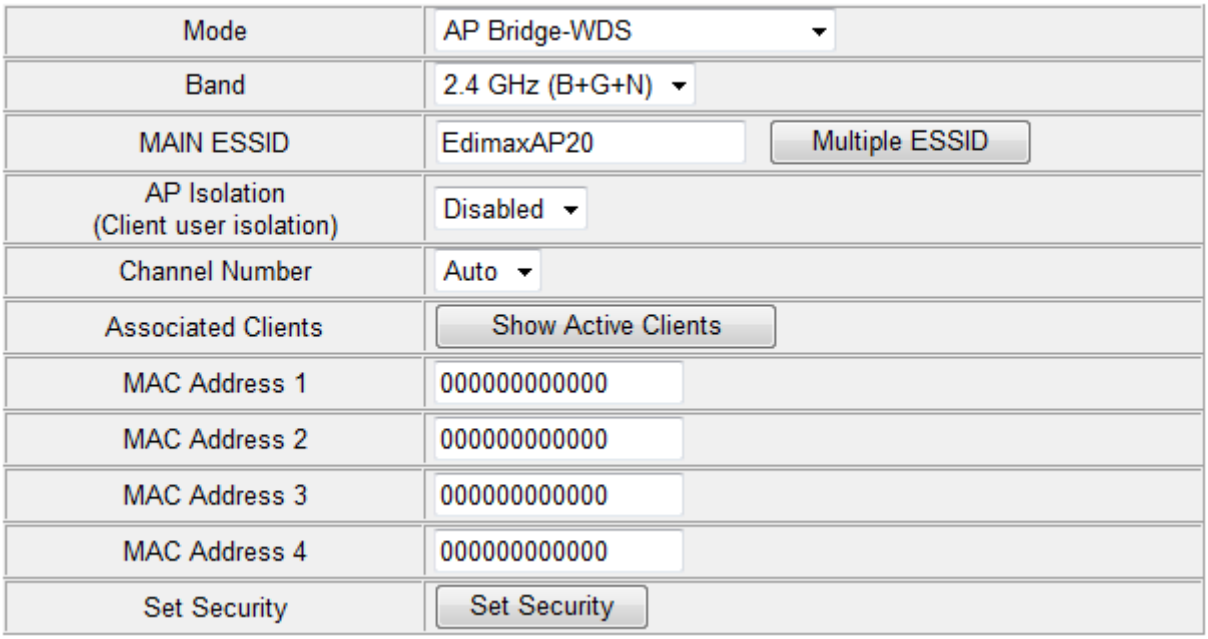
Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only access points of the same band or bands as you select will be able to connect.
Channel Number	Select a channel number for the access point. The channel number must be the same as the other access point you wish to connect to.
MAC Address 1-4	Enter MAC addresses of the wireless access point you wish to connect to.

Set Security	Click “Set Security” to select an encryption mode for this wireless link. A new window with security options will appear. See **III-5-1. Security.**

III-3-4. AP Bridge-WDS

In this mode, the access point can connect to up to four other wireless access points also using the same mode, and all connected Ethernet clients of all access points will be connected together. This allows several physically isolated networks to communicate with each other.

The access point can still accept wireless clients in this mode.



Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only access points of the same band or bands as you select will be able to connect.
MAIN ESSID	Specify an ESSID (the name used to identify the access point) of up to up to 32 alphanumerical characters. **Please note that the ESSID is case sensitive.**

Multiple ESSID	Click “Multiple ESSID” to open a new window and assign up to four ESSIDs to this access point. Please see the following page for more details.
AP Isolation	When this is set to “Enabled”, wireless clients connected to this device will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the MAIN ESSID only.
Channel Number	Select a channel number for the access point. The channel number must be the same as the other access point you wish to connect to.
Associated Clients	Click “Show Active Clients” to display a new window showing information about wireless clients.
MAC address 1-4	Enter MAC addresses of the wireless access point you wish to connect to.
Set Security	Click “Set Security” to select an encryption mode for this wireless link. A new window with security options will appear. See **III-5-1. Security.**

III-4. WPS Settings

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the device or from within the device's firmware/configuration interface. When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. PIN code WPS includes the use of a PIN code between the two devices for verification.

It is recommended to configure data encryption/security settings before using WPS.

WPS (Wi-Fi Protected Setup) Settings

This page allows you to configure WPS (Wi-Fi Protected Setup) settings. WPS allows wireless clients to connect to this device automatically.

☑ **Enable WPS**

- **Wi-Fi Protected Setup Information**

WPS Status:	Configured
Device PIN Code:	24555845
SSID:	EdimaxAP20
Authentication Mode:	WPA-Shared Key
Passphrase Key:	********

- **Device Configuration**

Config Mode:	Registrar
Configure via Push Button:	Start PBC
Input Client PIN Code :	Send PIN

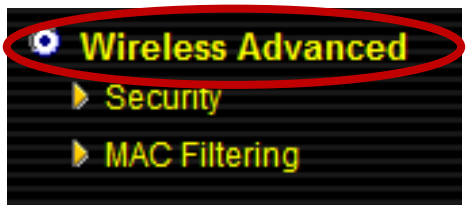
Enable WPS	Check/uncheck this box to enable/disable WPS

WPS Status	Displays “Configured” or “unConfigured” depending on whether WPS Settings for the access point have been configured or not, either manually or using the WPS button.
Device PIN Code	Displays the WPS PIN code of the access point.
SSID	Displays the SSID (ESSID) of the access point.
Authentication Mode	The wireless security authentication mode of the access point will be shown here. If you don’t enable the security functions of the access point before WPS is activated, the access point will automatically set the security to WPA (AES) and generate a passphrase key for WPS connection.
Passphrase Key	Displays the WPA passphrase, though all characters will be replaced by asterisks for security reasons. If encryption is not set on the access point, this field will be blank.
Config Mode	The configuration mode of the access point’s WPS setting is displayed here. “Registrar” means the device acts as an access point for a wireless client to connect to and the wireless client(s) will follow the access point’s wireless settings.
Configure via Push Button	Click “Start PBC” (Push-Button Configuration) to activate WPS on the access point. WPS will be active for 2 minutes.
Input Client PIN Code	Input the wireless client’s PIN code here and click “Start PIN” to activate PIN code WPS. Refer to your wireless client’s documentation if you are unsure of its PIN code.

For push-button configuration, please ensure you activate WPS on the wireless client within two minutes.

The access point’s green WPS LED will display on for five minutes to indicate a successful WPS connection.

III-5. Wireless Advanced



In “Wireless Advanced” you can configure advanced wireless settings. Please do not modify these settings unless you are sure of the effect these changes will have on your access point; advanced settings are for experienced users only.

Changing these settings can adversely affect the performance of your access point.

Wireless Advanced

These settings are only for more technical advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effects the changes will have.

Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
DTIM Period:	3 (1-10)
Data Rate:	Auto
N Data Rate:	Auto
Channel Width:	Auto 20/40MHz 20MHz
Preamble Type:	Short Preamble Long Preamble
Broadcast ESSID:	Enabled Disabled
WMM:	Enabled Disabled
CTS Protect:	Auto Always None
Tx Power:	100 %

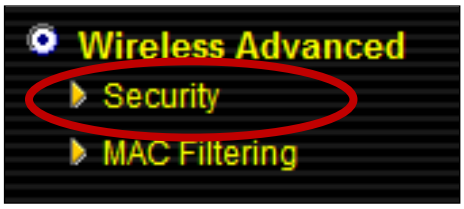
APPLY Cancel

Fragment Threshold	Set the Fragment threshold of the wireless radio. The default value is 2346.

RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
DTIM Period	Set the DTIM period of wireless radio. The default value is 3.
Data Rate	Set the wireless data transfer rate. The default is set to Auto.
N Data Rate	Set the data rate of 802.11n. The default is set to Auto .
Channel Width	Select wireless channel width (bandwidth used by wireless signals from the access point) – the recommended value is Auto 20/40MHz .
Preamble Type	Set the wireless radio preamble type. The default value is “Short Preamble”.
Broadcast ESSID	Set if the access point will broadcast its own ESSID. To hide the ESSID of your access point select “Disable” - only users who know the ESSID of your access point will be able to connect.
WMM	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When WMM is enabled, the access point will prioritize different kinds of data and give higher priority to applications which require instant responses. This improves the performance of such network applications.
CTS Protect	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It’s recommended to set this option to “Auto”.
TX Power	Set the power output of the wireless radio. Unless you’re using the access point in a very large space, you may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will

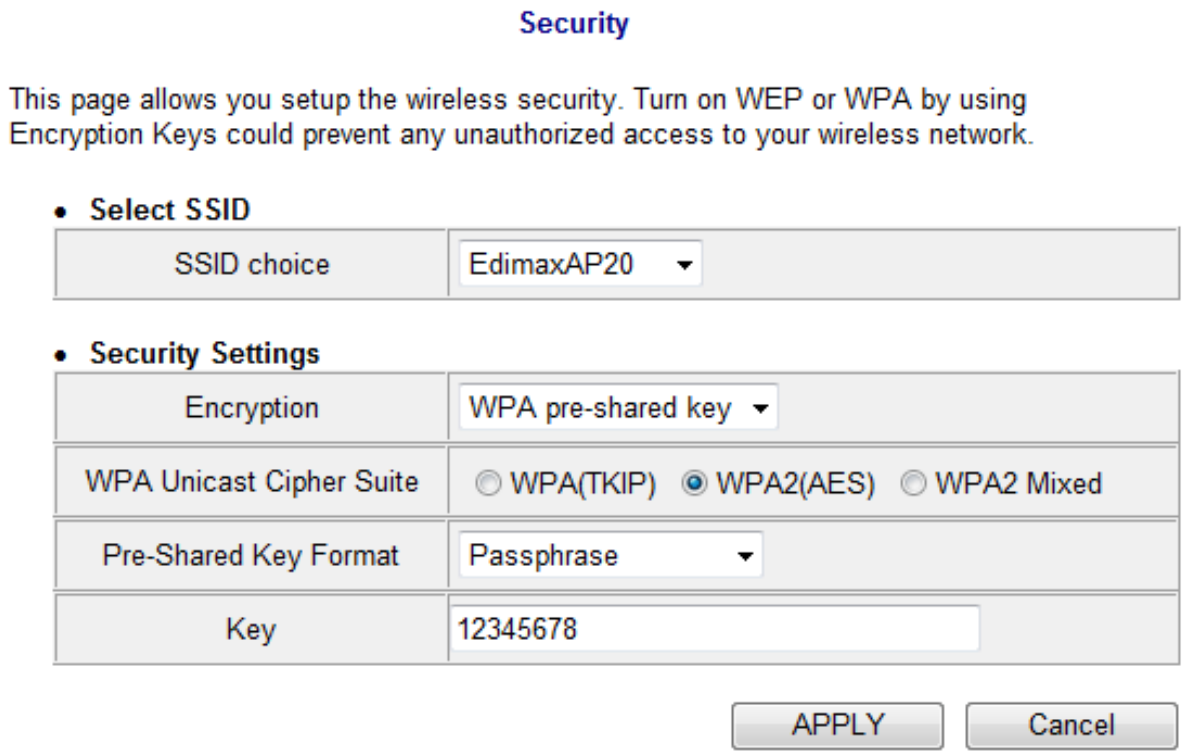
	not be able to access your signal.

III-5-1. Security



The access point provides a variety of wireless security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the encryption key.

Changing these settings can adversely affect the performance of your access point.



SSID choice	Select which SSID to configure security settings for.

Encryption	Select an SSID from the drop down menu to configure security for. Refer to the next section for more details about each security type.

III-5-1-1. Disable

When you select “Disable”, wireless encryption for the network is disabled.

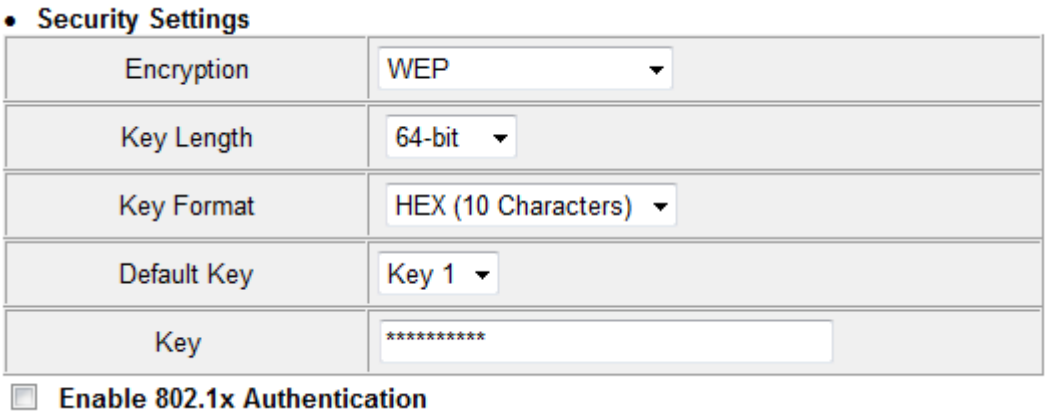
This setting is not recommended: anyone who knows your access point’s SSID can connect to it.

Enable 802.1x Authentication	Check this box to enable 802.1x user authentication. See **III-5-1-5. Enable 802.1x Authentication.**

III-5-1-2. WEP

WEP (Wired Equivalent Privacy) is a basic encryption type. For a higher level of security consider using WPA encryption.

Most wireless devices support WPA encryption, though some legacy devices only support WEP encyrption. WEP only supports data rates up to 54Mbps.

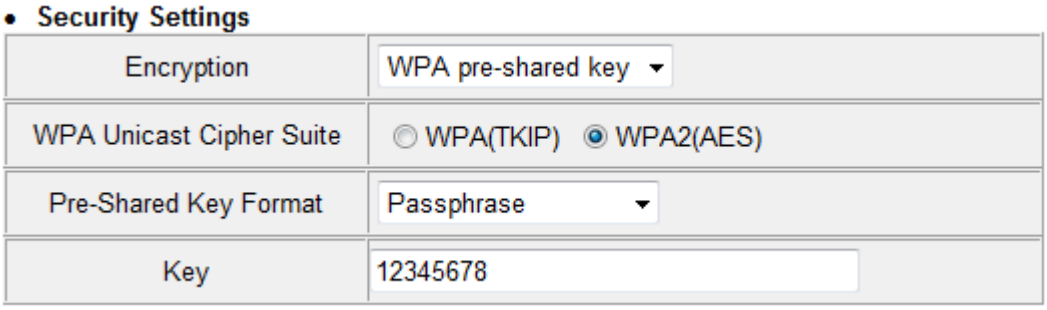


Key Length	There are two types of WEP key length: 64-bit and 128-bit. Using “128-bit” is safer than “64-bit”, but will reduce some data transfer performance.
Key Format	Select a key format: ASCII or Hex. The key length will also be displayed here - ASCII and Hex keys vary in length

	according to “Key Length” (above)”.
Default Key	You can set up to four sets of WEP keys, and you can decide which key is used the default. If you are unsure, leave the value as the default “Key 1”.
Key	Enter WEP key here, the number of characters must be the same as the number displayed in the “Key Format” field. For “ASCII” key format, you can use any alphanumerical characters (0-9, a-z, and A-Z). For “Hex” format, you can use the characters 0-9, a-f, and A-F. You must enter at least one encryption key here and if you enter multiple WEP keys, each should be unique.
Enable 802.1x Authentication	Check this box to enable 802.1x user authentication. See III-5-1-5. Enable 802.1x Authentication.

III-5-1-3. WPA Pre-Shared Key

WPA pre-shared key is the recommended and most secure encryption type.



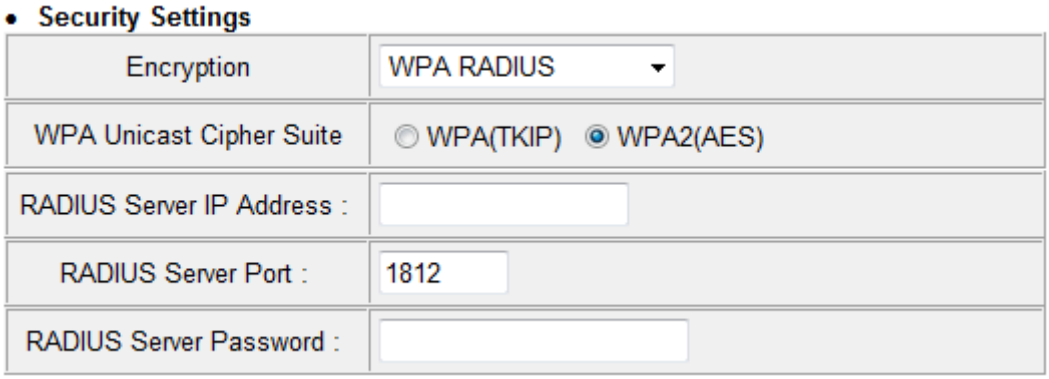
WPA (TKIP) only supports data rates up to 54Mbps.

WPA Unicast Cipher Suite	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. AES is safer than TKIP, but not supported by all wireless clients. Please make sure your wireless client supports your selection. WPA2(AES) is recommended, or WPA2 Mixed if

	your client does not support AES.
Pre-Shared Key Format	Select the pre-shared key format from “Passphrase” (8 to 63 alphanumerical characters) or “Hex (64 characters 0 to 9 and a to f.)
Key	Please enter the key according to the key format you selected above. For security reasons, it’s best to use a complex, hard-to-guess key.

III-5-1-4. WPA Radius

WPA RADIUS is a combination of WPA encryption and RADIUS user authentication. If you have a RADIUS authentication server, you can authenticate the identity of every wireless client against a user database.

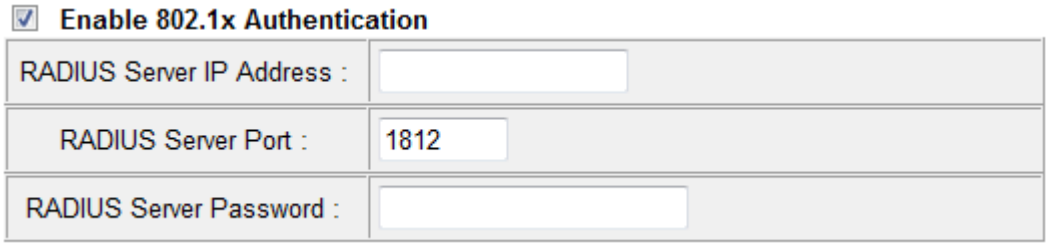


WPA Unicast Cipher Suite	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. AES is safer than TKIP, but not supported by all wireless clients. Please make sure your wireless client supports your selection. WPA2(AES) is recommended, or WPA2 Mixed if your client does not support AES.
Use internal MD5/PEAP RADIUS Server	Check the box to use an internal MD5/PEAP RADIUS Server.
RADIUS Server IP Address	Enter the IP address of the RADIUS authentication server here.
RADIUS Server Port	Enter the port number of the RADIUS authentication server here. Default value is

	1812.
RADIUS Server Password	Enter the password of the RADIUS authentication server here.

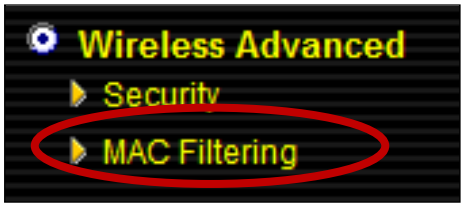
III-5-1-5. Enable 802.1x Authentication

If you select “Disable” or “WEP” as your encryption type, you can check the “Enable 802.1x Authentication” box to enable 802.1x authentication based on a RADIUS user authentication server.

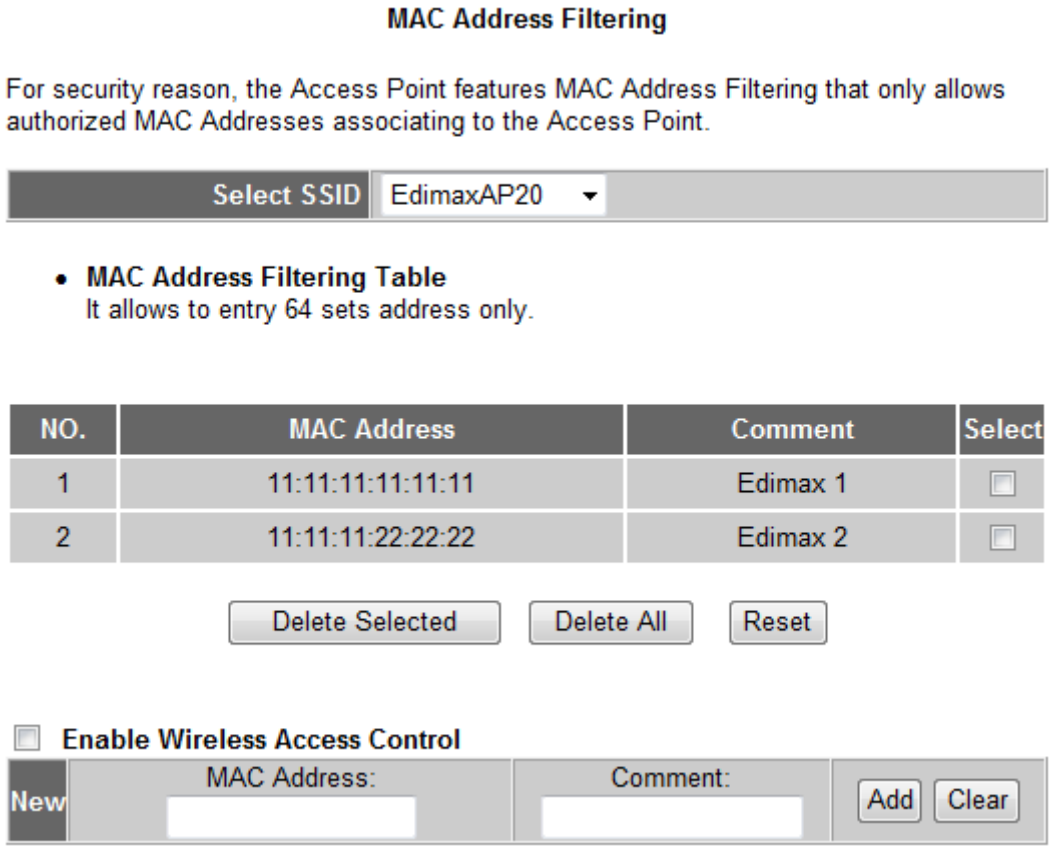


Enable 802.1x Authentication	Enable or disable the use of 802.1x user authentication.
RADIUS Server IP Address	Enter the IP address of the RADIUS authentication server here.
RADIUS Server Port	Enter the port number of the RADIUS authentication server here. Default value is 1812.
RADIUS Server Password	Enter the password of the RADIUS authentication server here.

III-5-2. MAC Filtering



The MAC filtering feature allows you to define a list of wireless devices permitted to connect to this access point, identified by their unique MAC address. When this feature is enabled, devices which are not on the list of permitted MAC addresses cannot connect to the access point.



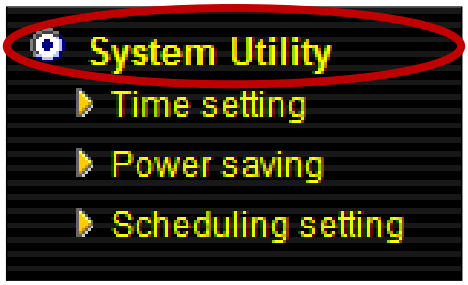
SSID choice	Select which SSID to configure MAC address filtering.

Select	Check this box to select MAC address(es).
Delete Selected	Click this button to delete selected MAC address(es).
Delete All	Delete all MAC addresses in the table.
Reset	Uncheck all selected MAC address entries.

Enable Wireless Access Control	Check this box to enable MAC address filtering.

MAC address	Enter a MAC address permitted to connect to the access point. Only enter characters 0 to 9 or a to f.
Comment	Enter an optional comment associated with the specified MAC address for reference/identification, consisting of up to 16 alphanumerical characters.
Add	Add the MAC address entry to the list.
Clear	Remove all characters in the “MAC address” and “Comments” fields.

III-6. System Utility



In “System Utility” you can configure basic system and administrative parameters.

Administrator

If you wish to customize the login information for your Access Point, please enter the new user name and password in the following columns.If you want to set up a DHCP server, you need to assign this device an unique IP address.

- **Password Settings**

Current Password :	
New Password :	
Re-Enter Password :	

- **Management IP**

Obtain an IP address automatically	
Use the following IP address	
IP Address :	192.168.2.2
Subnet Mask :	255.255.255.0
Gateway Address :	

- **DHCP Server**

DHCP Server :	Disabled
Default Gateway :	192.168.2.2
Start IP :	192.168.2.100
End IP :	192.168.2.200
Lease Time :	Forever

You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.

If you change the administrator password, please make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface, see II-2. Reset for how to reset the access point.

Current Password	Enter your current password. The default password is **1234**.
New Password	Enter your desired new password here. You can use any combination of letters, numbers and symbols up to 20 characters.
Re-Enter Password	Confirm your new password.

Please refer to IV-1. Configuring your IP address for more information about changing the access point's IP address.

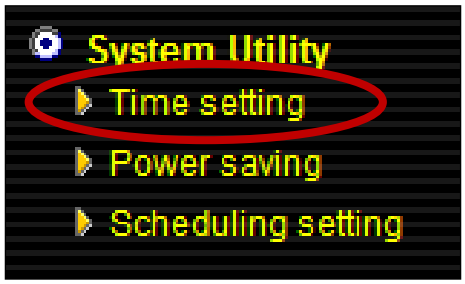
IP Address	Specify an IP address here. This IP address will be assigned to your access point, and will replace the default IP address 192.168.2.2.
Subnet Mask	Input the subnet mask of the new IP address.
Gateway Address	Input the network's gateway IP address.

The access point can be configured to act as a DHCP server for your network. By default DHCP is disabled. Enable DHCP by selecting "Enable" in the field "DHCP Server" of "Management IP" as detailed in the previous section.

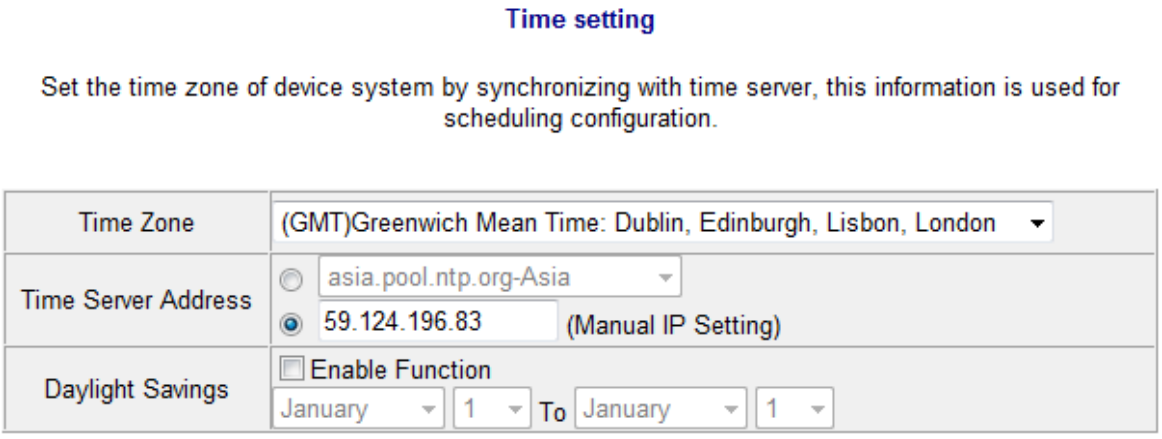
DHCP Server	Select "Enabled" if you wish to use the DHCP function of the access point, as detailed below.
Default Gateway	Specify the IP address of the default gateway of your network here.
Start IP	Enter the start address of the IP range.
End IP	Enter the end address of the IP range.
Domain Name	Enter the domain name for your network (optional).
Lease Time	Choose a lease time (the duration that every computer can keep a specific IP address) of

	every IP address assigned by the access point.

III-6-1. Time Setting

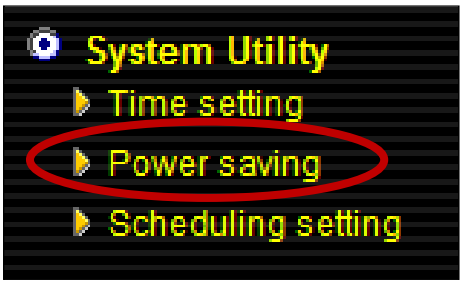


You can configure the time zone settings of your access point here. The date and time of the device can be configured manually or can be synchronized with a time server.



Time Zone	Select the time zone of your country/ region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.
Time Server Address	This access point supports NTP (Network Time Protocol) for automatic time and date setup. Choose a time server from the drop down menu, or input the host name or IP address of the IP server manually.
Daylight Savings	If your country/region uses daylight saving time, please check the “Enable Function” box and select the start and end date.

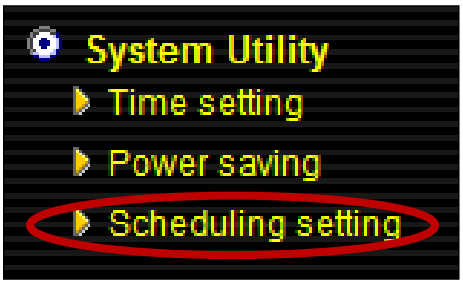
III-6-2. Power Saving



You can configure the access point's LEDs in order the conserve power.

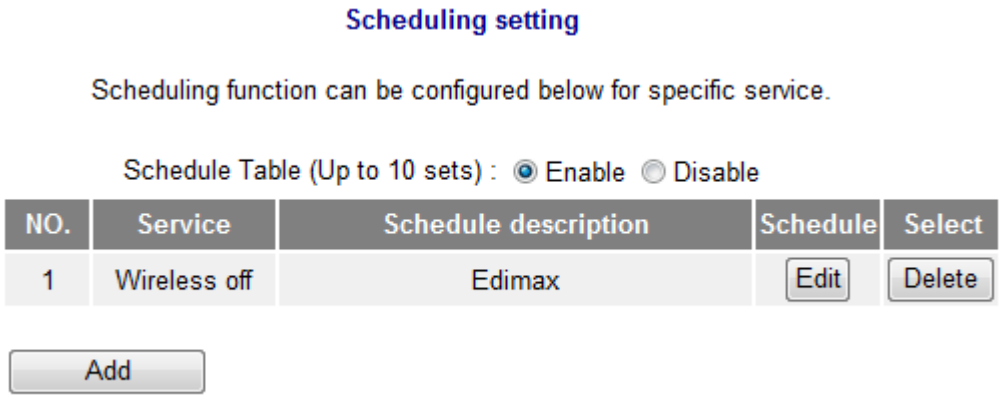
LED ON/OFF	Select "ON" or "OFF" to switch the LEDs on or off accordingly.

III-6-3. Scheduling Setting



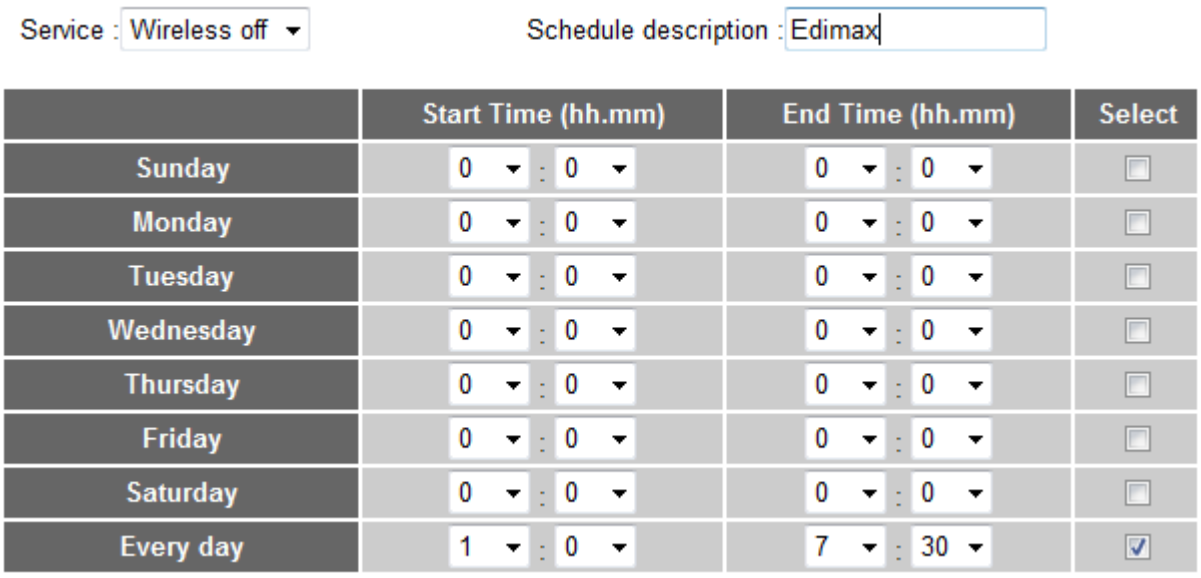
The access point includes a scheduling function, where power saving functions and an automatic reboot can be automated for specific times. By default, scheduling setting is disabled. Please select “Enable” if you wish to continue.

Ensure you have configured the time settings of your access point before you enable scheduling.


Scheduling setting
Scheduling function can be configured below for specific service.
Schedule Table (Up to 10 sets) : Enable Disable
NO. Service Schedule description Schedule Select
1 Wireless off Edimax Edit Delete
Add

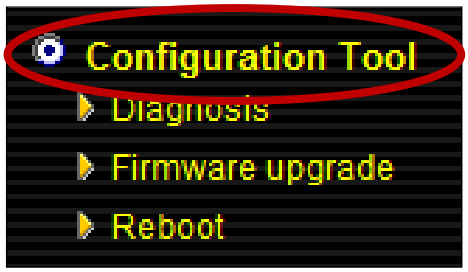
Up to 10 events can be scheduled.

Add	Open a new screen and create a scheduled event.
Edit	Click “Edit” to change the type, description, start time or end time of the scheduled event.
Delete	Click “Delete” to delete the event permanently.

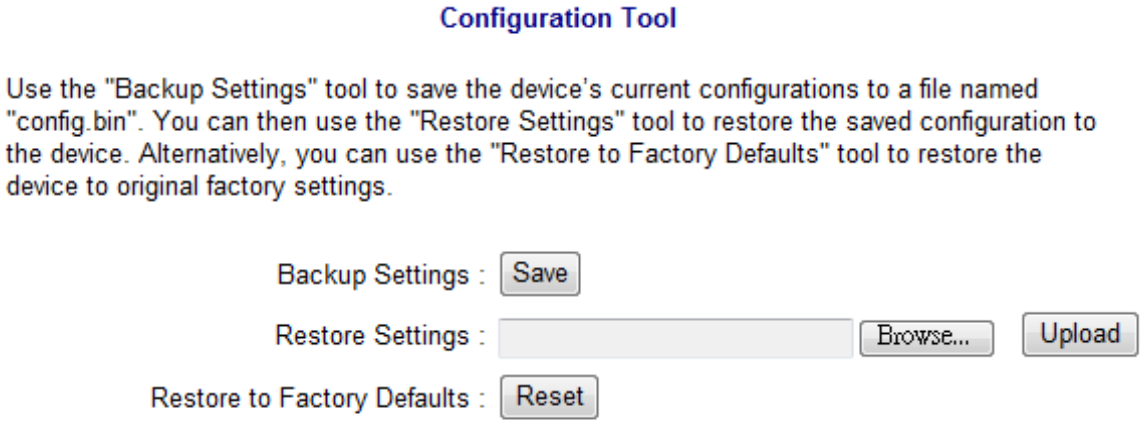

Service : Wireless off
Schedule description : Edimax
Start Time (hh.mm)
End Time (hh.mm)
Select
Sunday 0 : 0 0 : 0
Monday 0 : 0 0 : 0
Tuesday 0 : 0 0 : 0
Wednesday 0 : 0 0 : 0
Thursday 0 : 0 0 : 0
Friday 0 : 0 0 : 0
Saturday 0 : 0 0 : 0
Every day 1 : 0 7 : 30

Service	Select the event to be scheduled from the drop down menu. “Wireless off” will disable the wireless capability of the access point, “Led off” will switch off the LEDs and “Auto reboot” will restart the device.
Schedule Description	Assign the event a name or description for reference (optional).
Start Time	Specify a start time (hh.mm) for the event, for a specific day or to recur every day.
End Time	Specify an end time (hh.mm) for the event, for a specific day or to recur every day.
Select	Check the box to select and confirm your event.

III-7 Configuration Tool

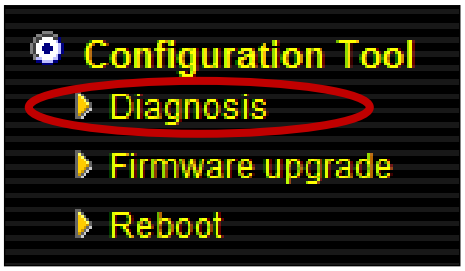


The access point's configuration tool enables you to back up the settings, upgrade the firmware and reset the device. Select "Configuration tool" from the sidebar.

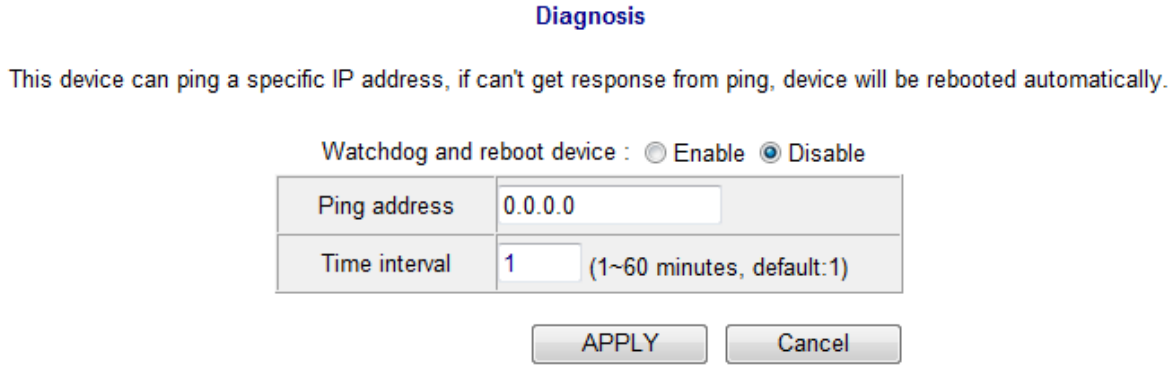

Configuration Tool
Use the "Backup Settings" tool to save the device's current configurations to a file named "config.bin". You can then use the "Restore Settings" tool to restore the saved configuration to the device. Alternatively, you can use the "Restore to Factory Defaults" tool to restore the device to original factory settings.
Backup Settings : Save
Restore Settings : Browse... Upload
Restore to Factory Defaults : Reset

Backup Settings	Click "Save" to save the current settings on your computer as config.bin file.
Restore Settings	Click the browse button to find a previously saved config.bin file and then click "Upload" to replace your current settings.
Restore to Factory Defaults	Click "Reset" to restore settings to the factory default. A pop-up window will appear and ask you to confirm and enter your log in details. Enter your username and password and click "Ok". See below for more information.

III-7-1. Diagnosis

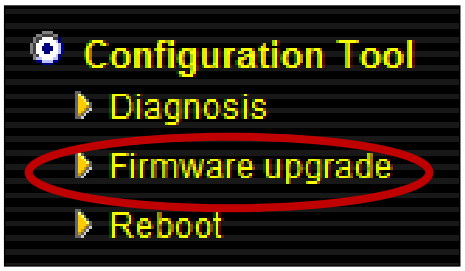


Using the diagnosis tool, you can ping a specific IP address and automatically reboot the device if there is no response.



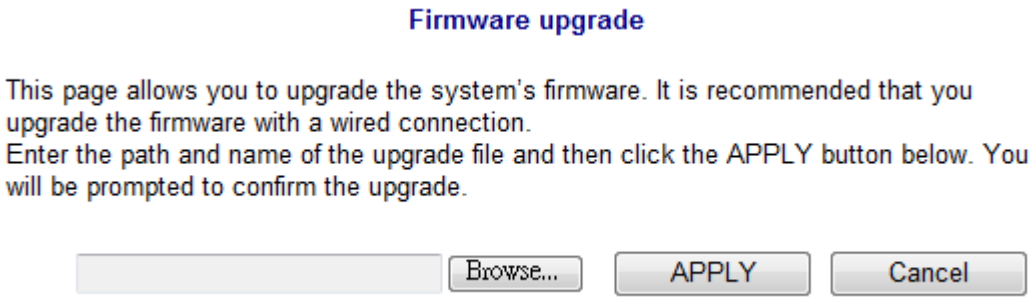
Watchdog and reboot device	Select “Enable” or “Disable” for the automatic reboot function.
Ping Address	Specify the IP address to ping.
Time interval	Specify the frequency of the ping as a time interval, in minutes. Enter a value from 1-60.

III-7-2. Firmware Upgrade



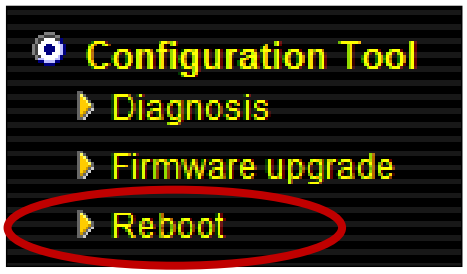
Selecting “Firmware upgrade” from the “Configuration Tool” menu allows you to update the system firmware to a more recent version. You can download the latest firmware from the Edimax website.

Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.


Firmware upgrade
This page allows you to upgrade the system's firmware. It is recommended that you upgrade the firmware with a wired connection.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.
Browse...
APPLY
Cancel

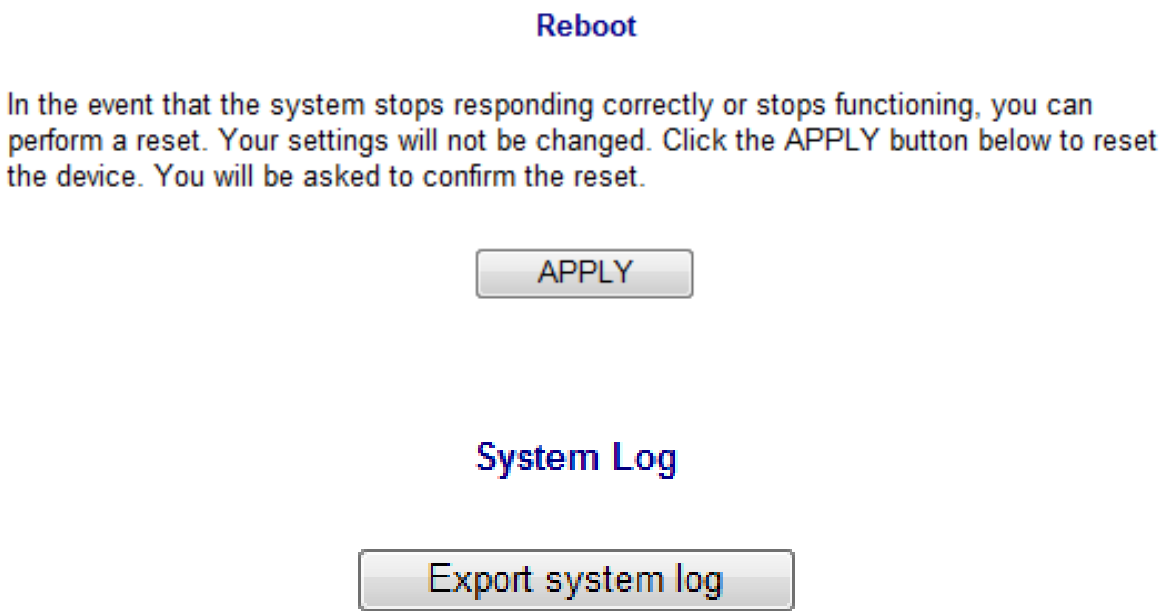
Browse	Open a new window to locate and select the firmware file in your computer.

III-7-3. Reboot



If the access point malfunctions or is not responding, then it is recommended that you reboot the device. You can reboot the access point remotely using this feature if the location of the access point is not convenient. You can also export the access point's system log.

Rebooting the access point will not affect the current configuration/settings of the device.


Reboot
In the event that the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. Click the APPLY button below to reset the device. You will be asked to confirm the reset.
APPLY
System Log
Export system log

Apply	Click "Apply" to reboot the device. A status bar will indicate the progress of the reboot and you will see a confirmation screen when the reboot is complete.

Export system log	Click to open a new window and select a location to save the log file.

IV. Appendix

IV-1. Configuring your IP address

For first-time access, the URL** http://EdimaxAP** **will not work for static IP users.

For first time access to the URL *http://EdimaxAP** your computer must be set to use a dynamic IP address. This means your computer can obtain an IP address automatically from a DHCP server. You can check if your computer is set to use a dynamic IP address by following **IV-1-1. How to check that your computer uses a dynamic IP address**.

Static IP users can use the access point's default IP address **192.168.2.2** instead. But in order to do so, you need to temporarily modify your computer's IP address to be in the same IP address subnet e.g. **192.168.2.x (x = 3 – 254).**

The procedure for modifying your IP address varies across different operating systems; please follow the guide appropriate for your operating system in **IV-1-2. How to modify the IP address of your computer**.

Static IP users please make a note of your static IP before you change it.

You can assign a new IP address to the access point which is within the subnet of your network using the browser based configuration interface (refer to **III-6. System Utility**). Then static IP users can also use the URL *http://EdimaxAP** for future access to iQ Setup or the browser based configuration interface.

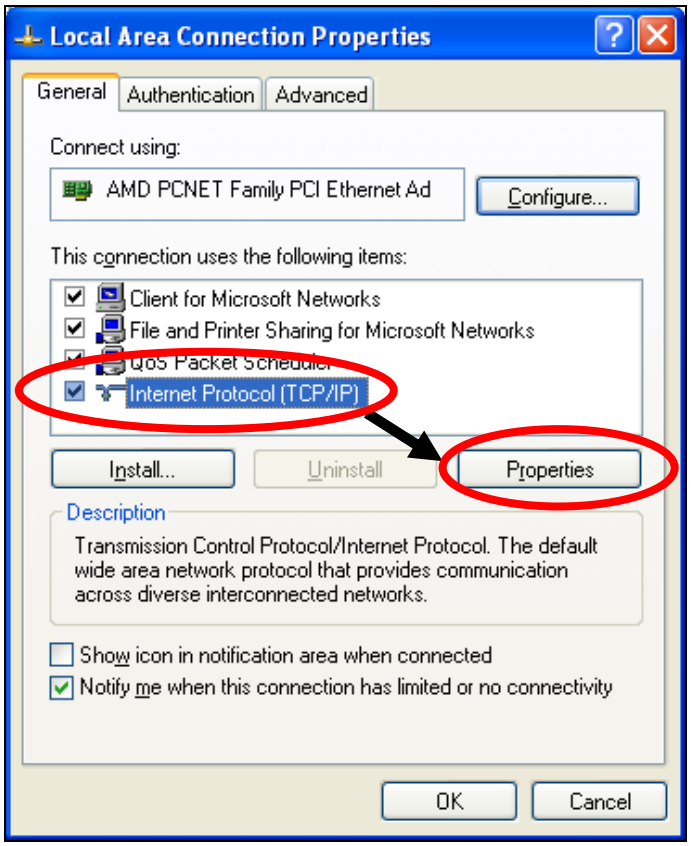
Please remember to change your IP address back to its original value after the access point is properly configured.

IV-1-1. How to check that your computer uses a dynamic IP address

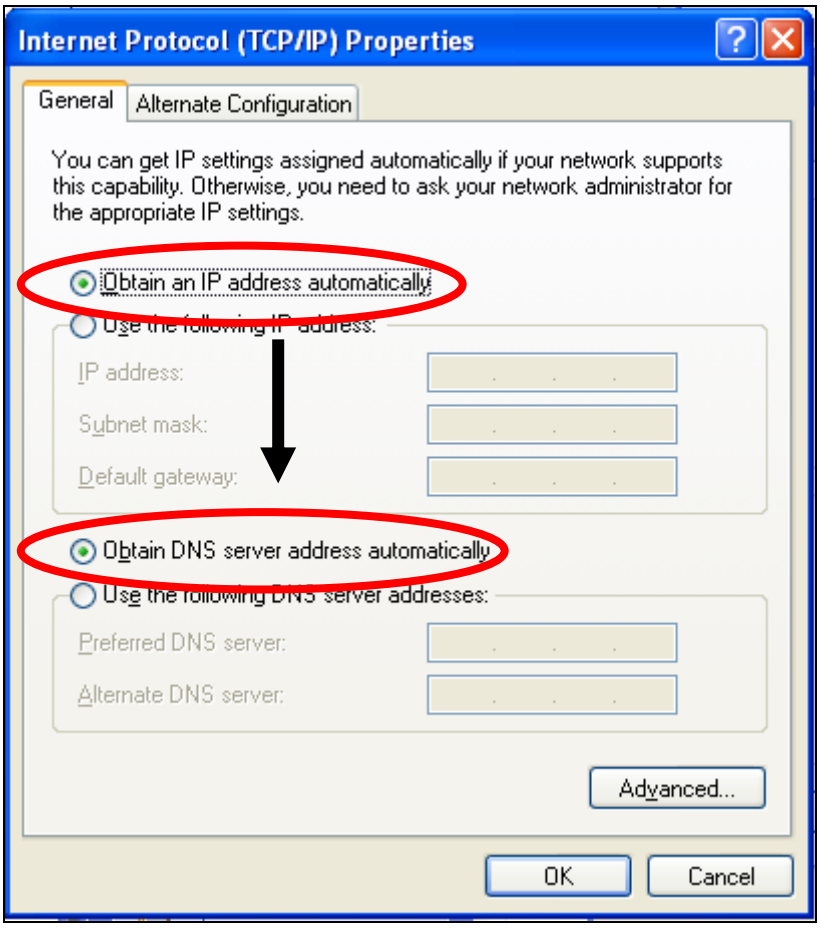
Please follow the instructions appropriate for your operating system.

IV-1-1-1. Windows XP

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Double-click the “Network and Internet Connections” icon, click “Network Connections”, and then double-click “Local Area Connection”. The “Local Area Connection Status” window will then appear, click “Properties”.

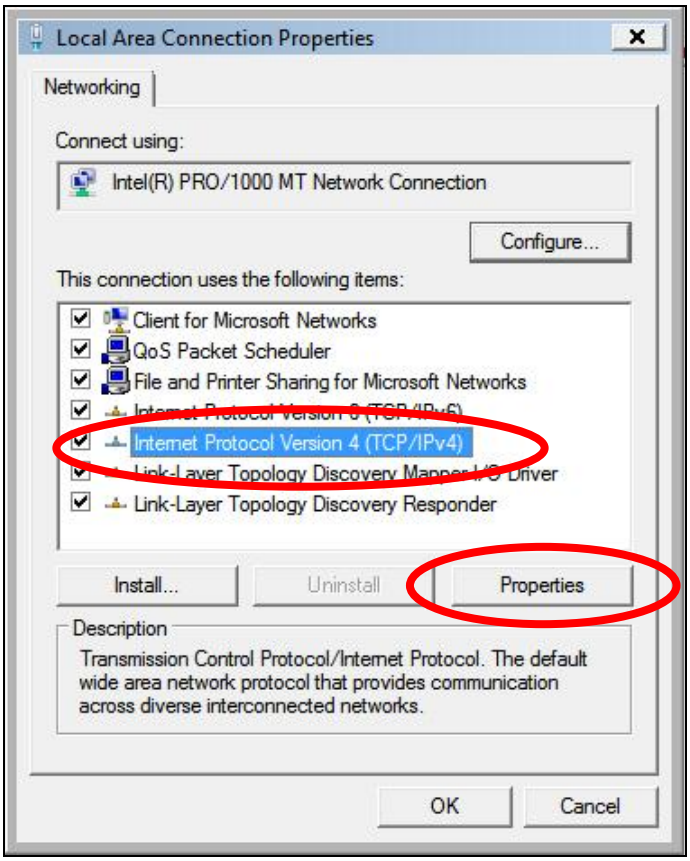


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.

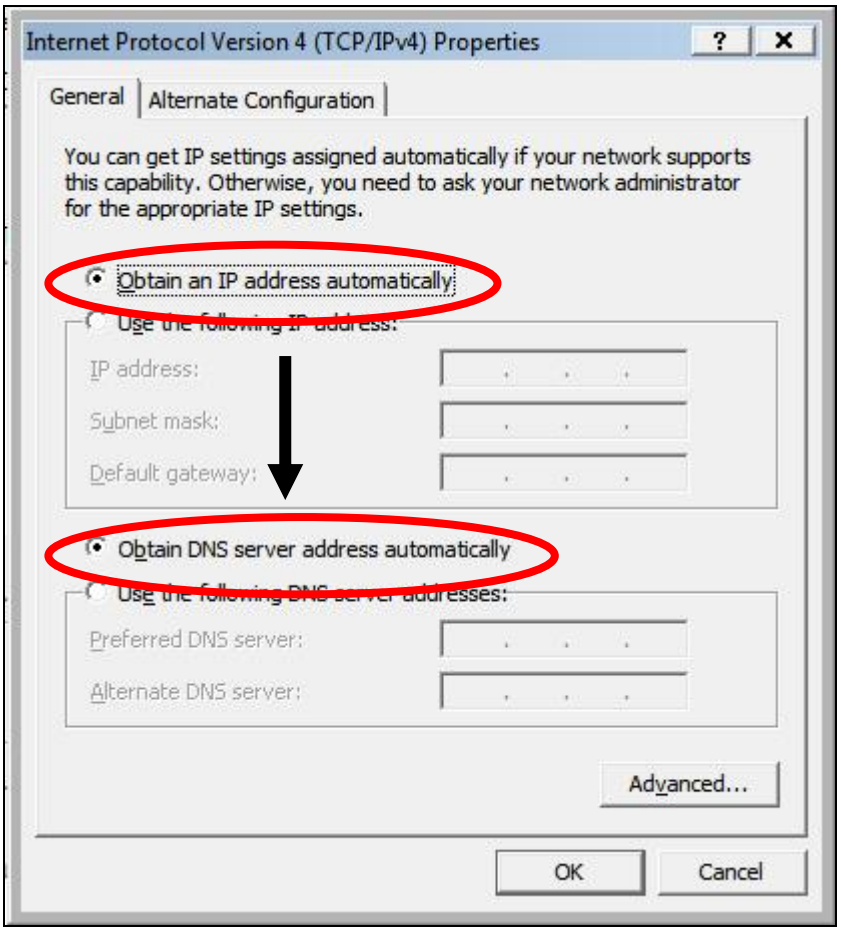

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

IV-1-1-2. Windows Vista

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Click “View Network Status and Tasks”, then click “Manage Network Connections”. Right-click “Local Area Network”, then select “Properties”. The “Local Area Connection Properties” window will then appear, select “Internet Protocol Version 4 (TCP / IPv4)”, and then click “Properties”.

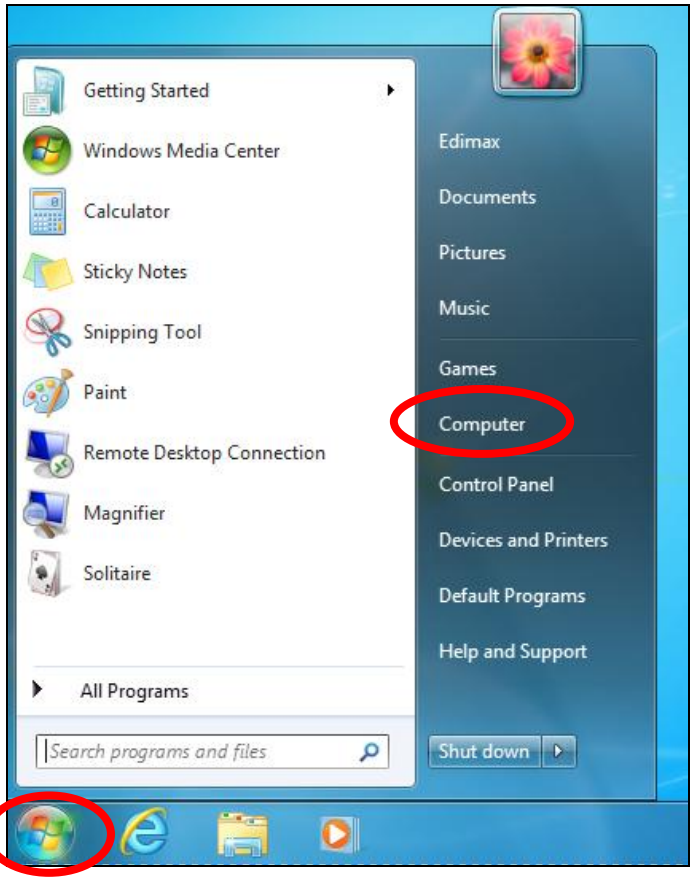


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.

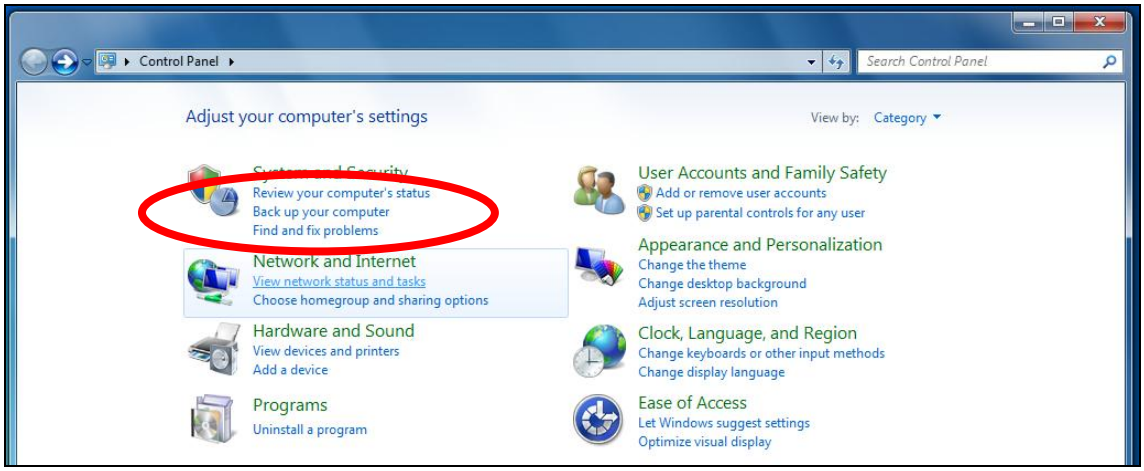

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

IV-1-1-3. Windows 7

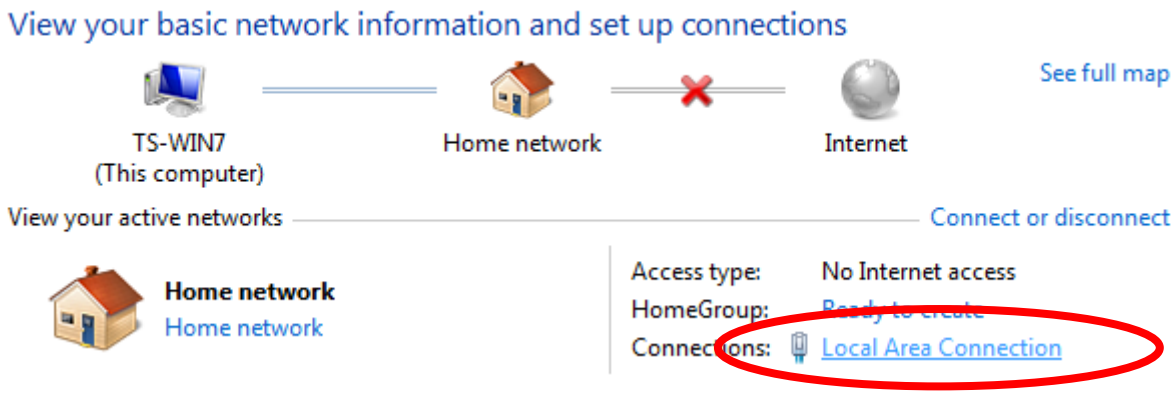
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



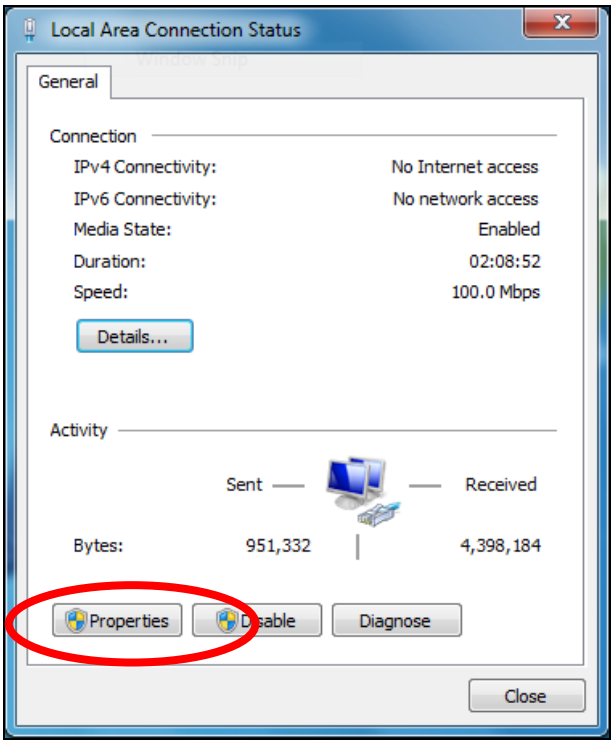
2. Under “Network and Internet” click “View network status and tasks”.



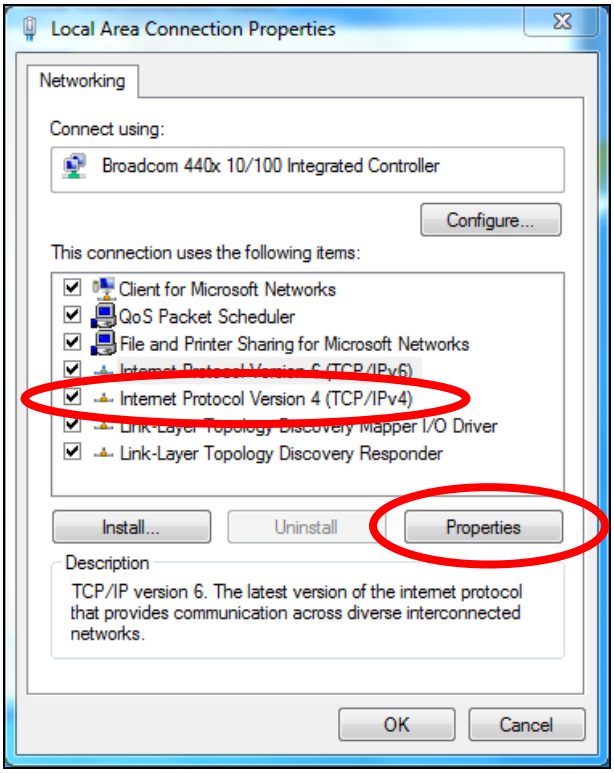
3. Click “Local Area Connection”.



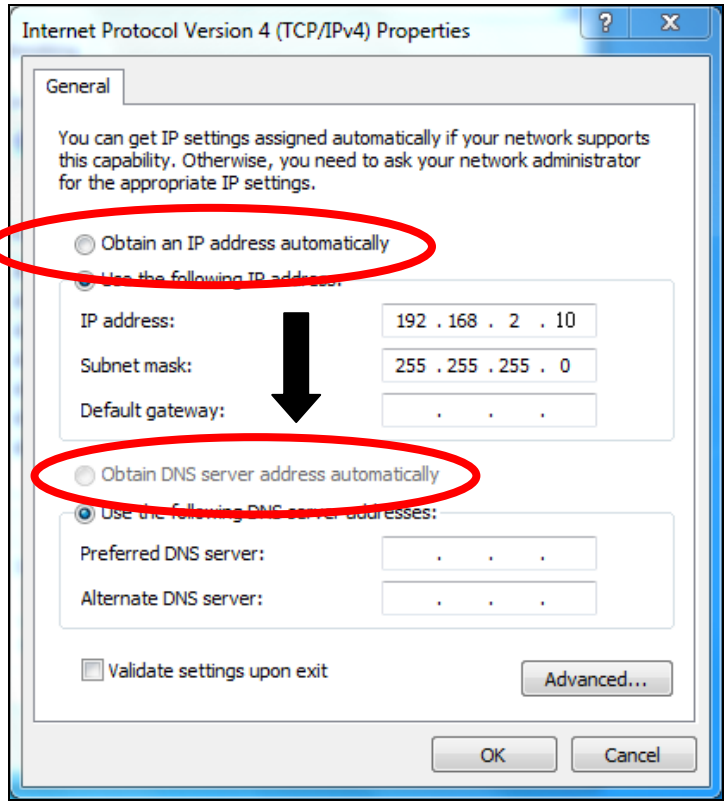
4. Click “Properties”.



5. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.

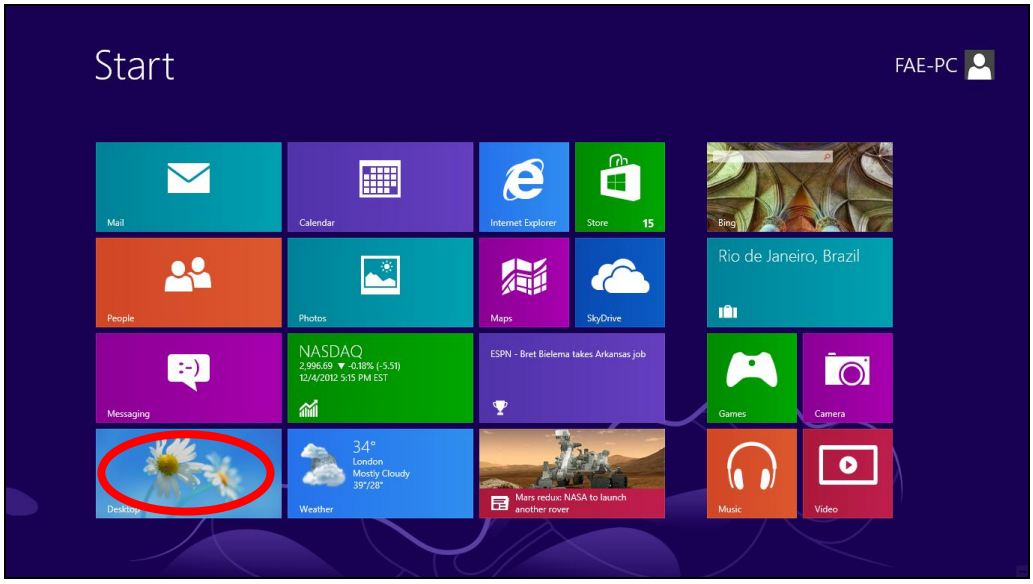


6. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.

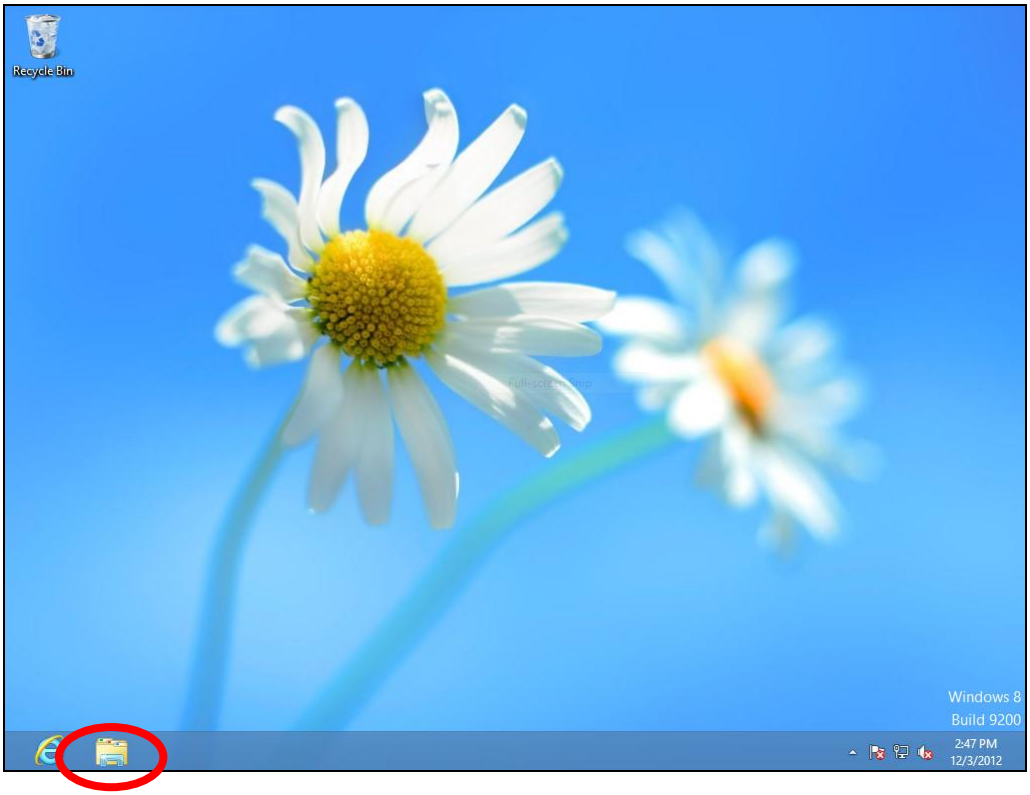

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
IP address:
192 . 168 . 2 . 10
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

IV-1-1-4. Windows 8

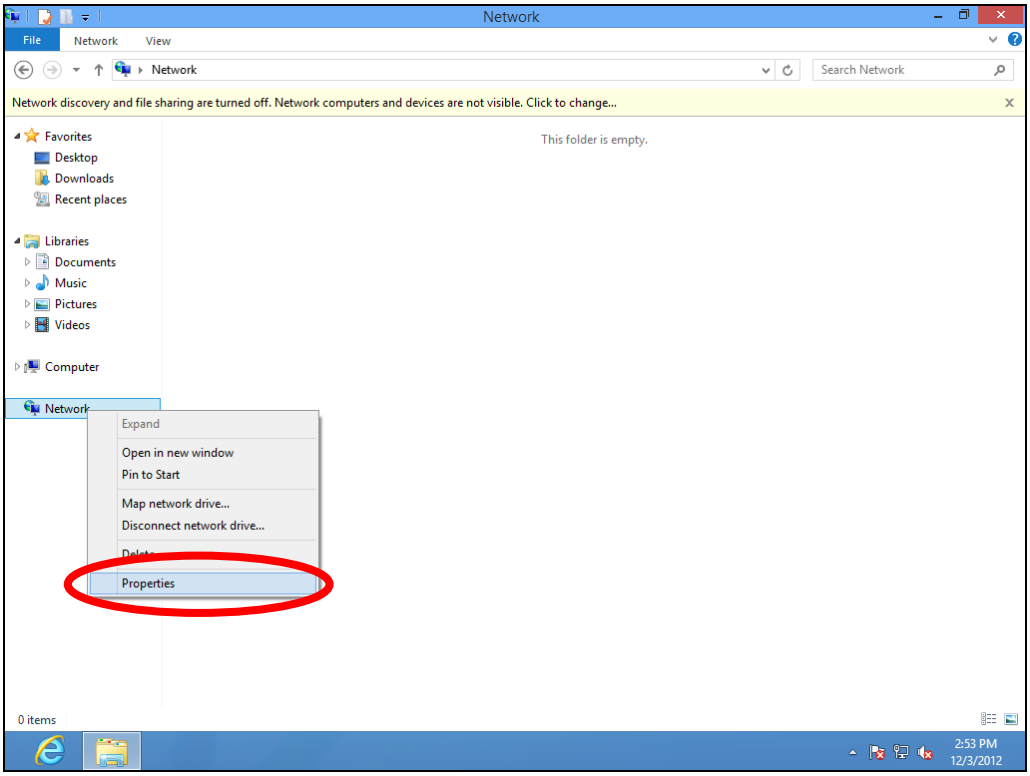
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your curser to the bottom left of the screen and click.



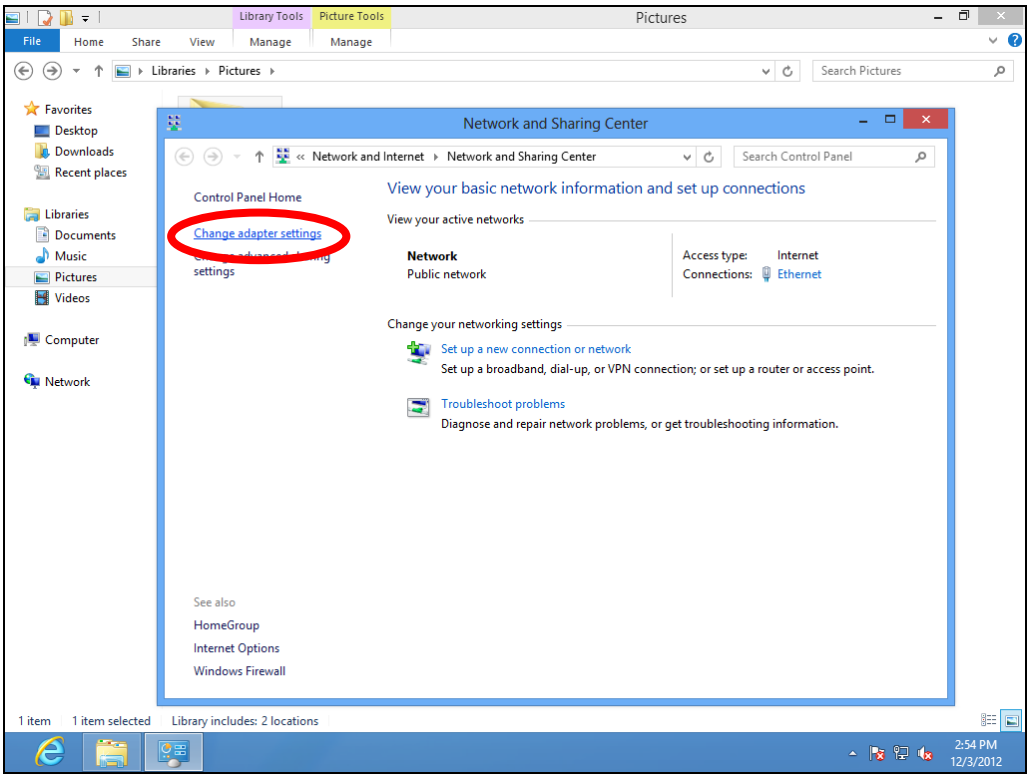
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



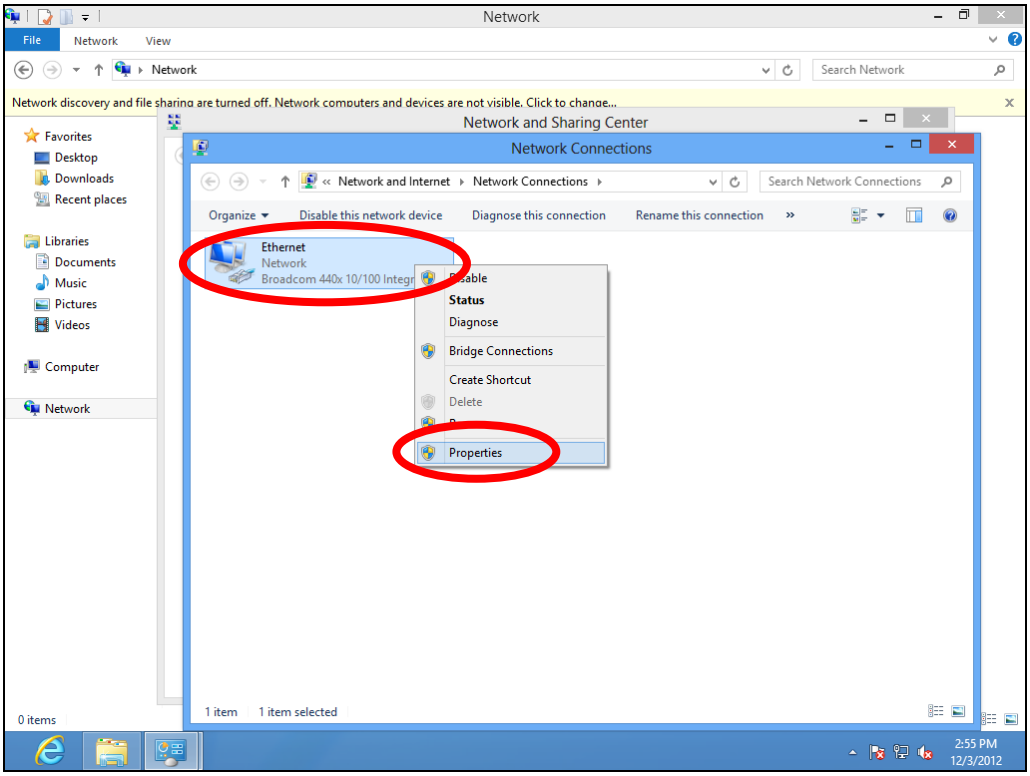
3. Right click “Network” and then select “Properties”.



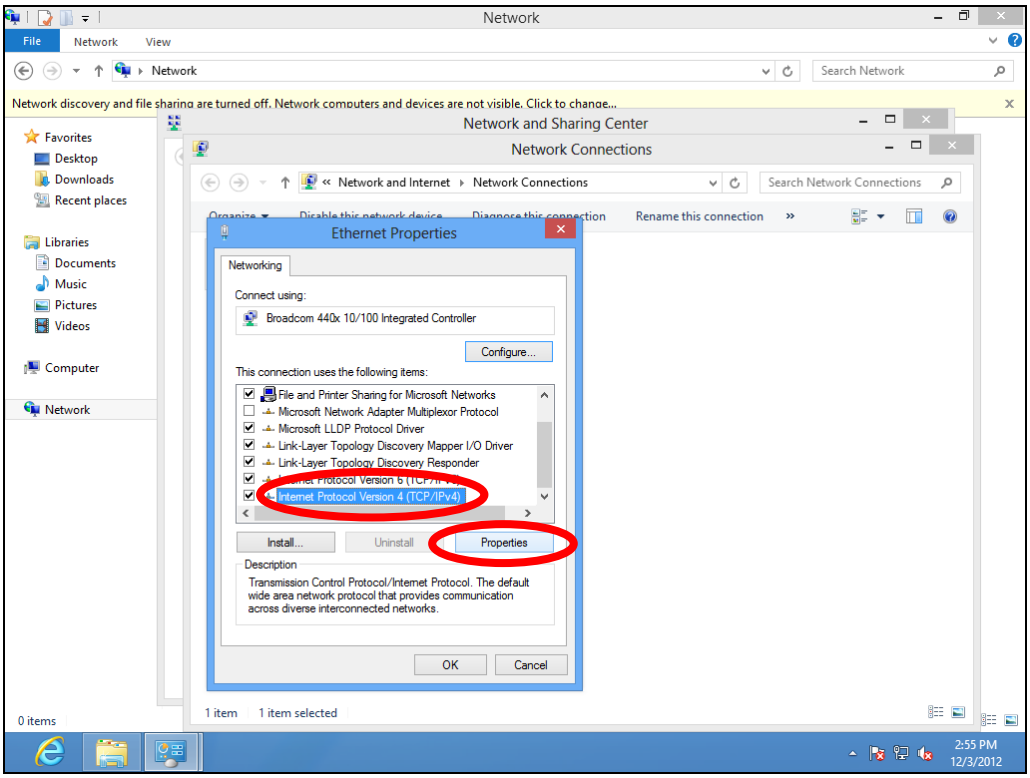
4. In the window that opens, select “Change adapter settings” from the left side.



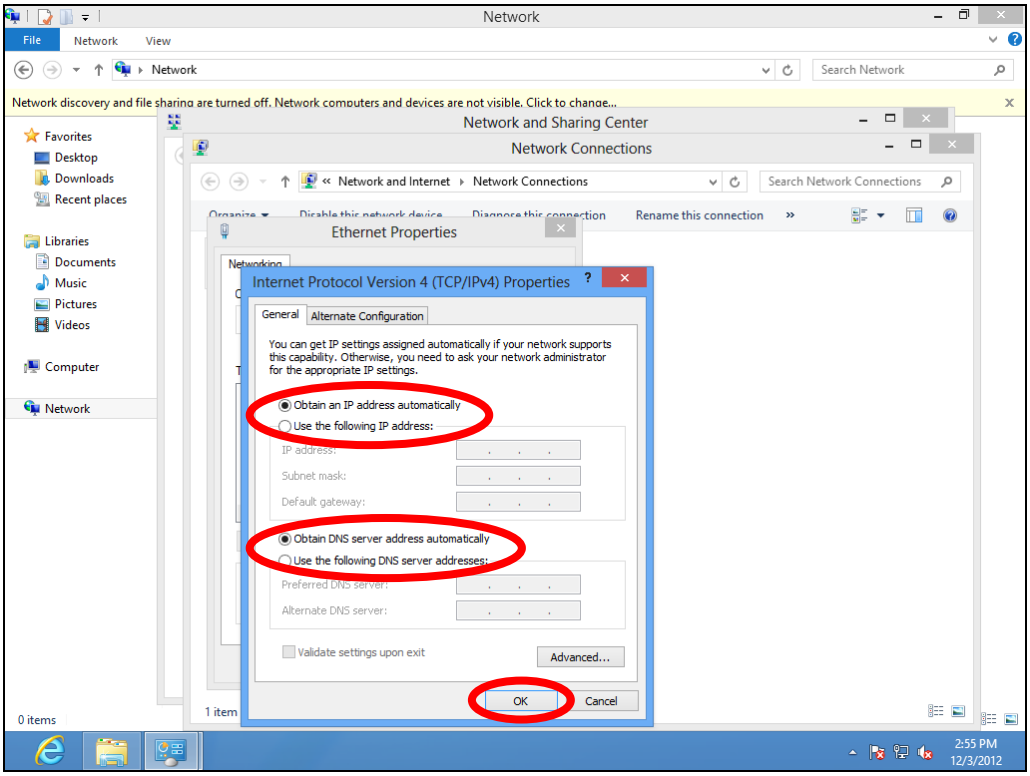
5. Choose your connection and right click, then select “Properties”.



6. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.



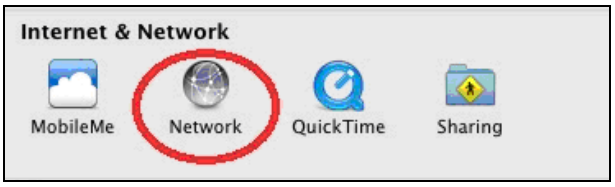
7. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.


Network
File
Network
View
Network
Search Network
Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...
Favorites
Desktop
Downloads
Recent places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
0 items
Network and Sharing Center
Network Connections
Network and Internet
Network Connections
Search Network Connections
Rename this connection
Ethernet Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
1 item
2:55 PM
12/3/2012

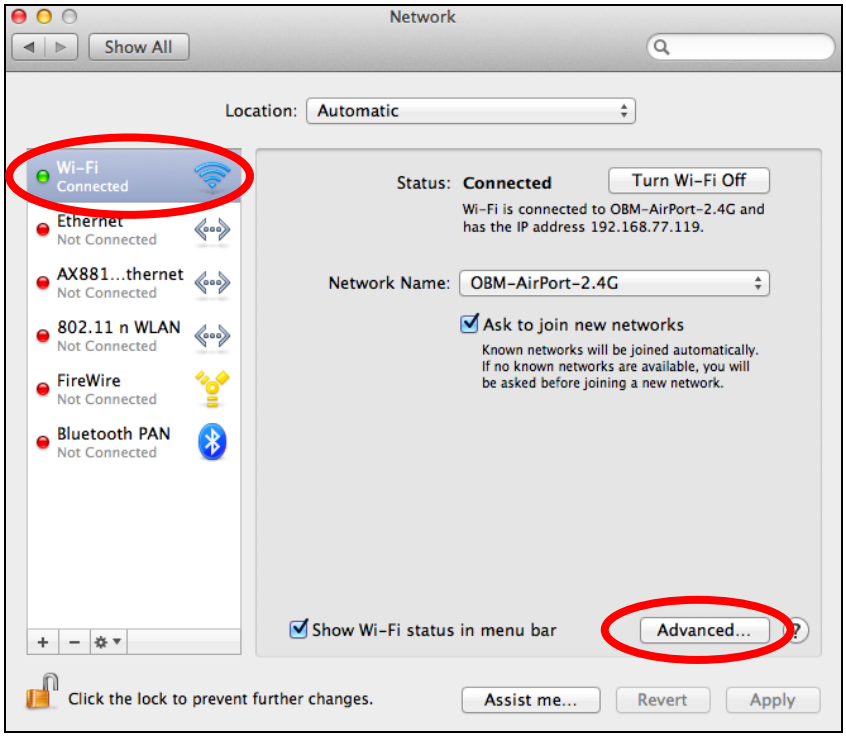
IV-1-1-5. Mac OS

1. Have your Macintosh computer operate as usual, and click on “System Preferences”.

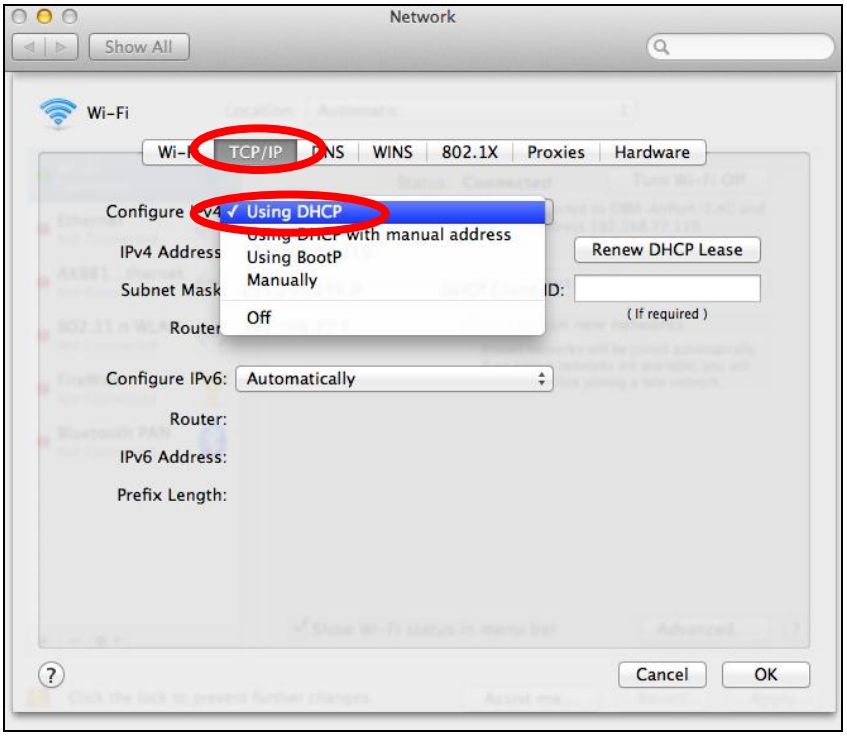
2. In System Preferences, click on “Network”.



3. Click on “Wi-Fi” in the left panel and then click “Advanced” in the lower right corner.



4. Select “TCP/IP” from the top menu and “Using DHCP” in the drop down menu labeled “Configure IPv4” should be selected.


Network
Show All
Wi-Fi
TCP/IP
DNS
WINS
802.1X
Proxies
Hardware
Using DHCP
Using BootP
Manually
Off
Renew DHCP Lease
(If required)
Configure IPv6:
Automatically
Router:
IPv6 Address:
Prefix Length:
Cancel
OK

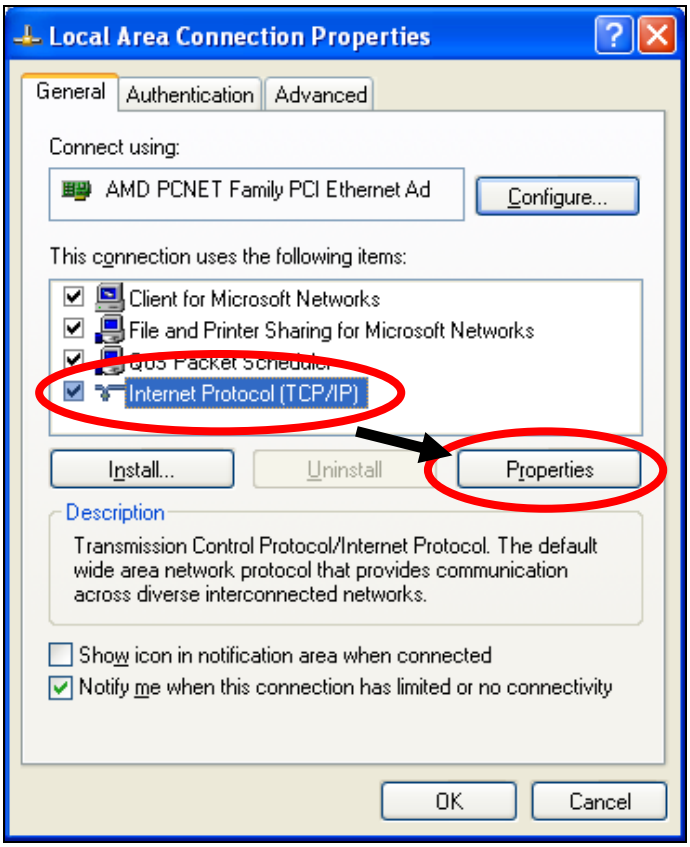
IV-1-2. How to modify the IP address of your computer

Please follow the instructions appropriate for your operating system. In the following examples we use the IP address **192.168.2.10** though you can use any IP address in the range **192.168.2.x (x = 3 – 254)** in order to access iQ Setup/browser based configuration interface.

Please make a note of your static IP before you change it.

IV-1-2-1. Windows XP

1. Click the "Start" button (it should be located in the lower-left corner of your computer), then click "Control Panel". Double-click the "Network and Internet Connections" icon, click "Network Connections", and then double-click "Local Area Connection". The "Local Area Connection Status" window will then appear, click "Properties".



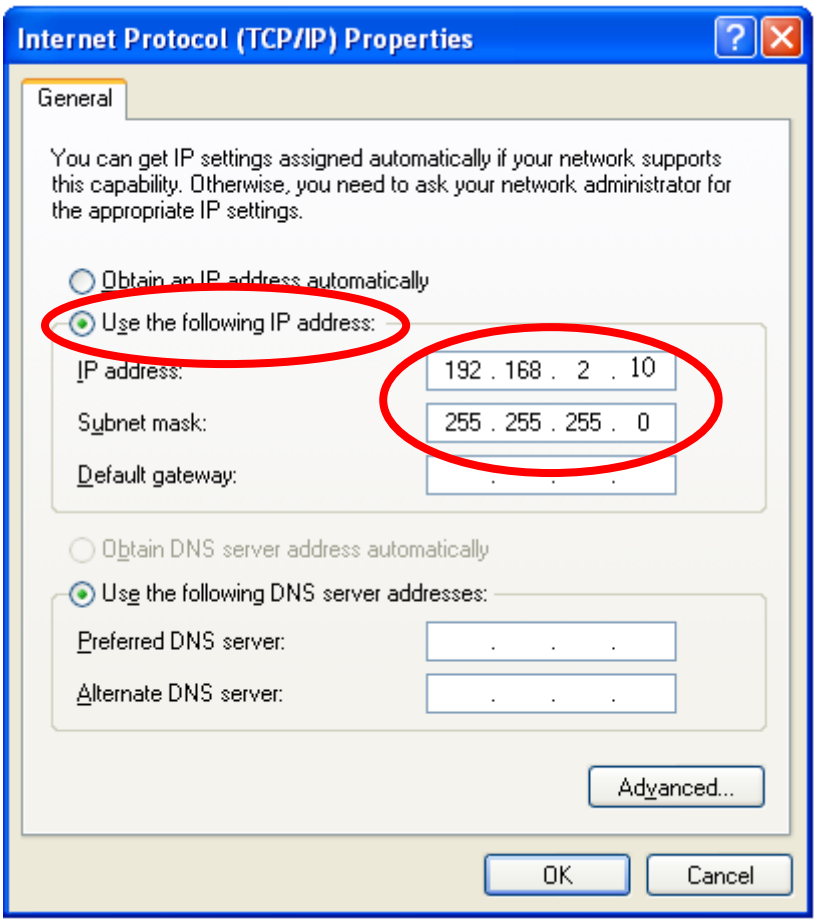
2. Select "Use the following IP address", then input the following values:

Your existing static IP address will be displayed in the "IP address" field before you replace it. Please make a note of this IP

address, subnet mask, default gateway and DNS server addresses.

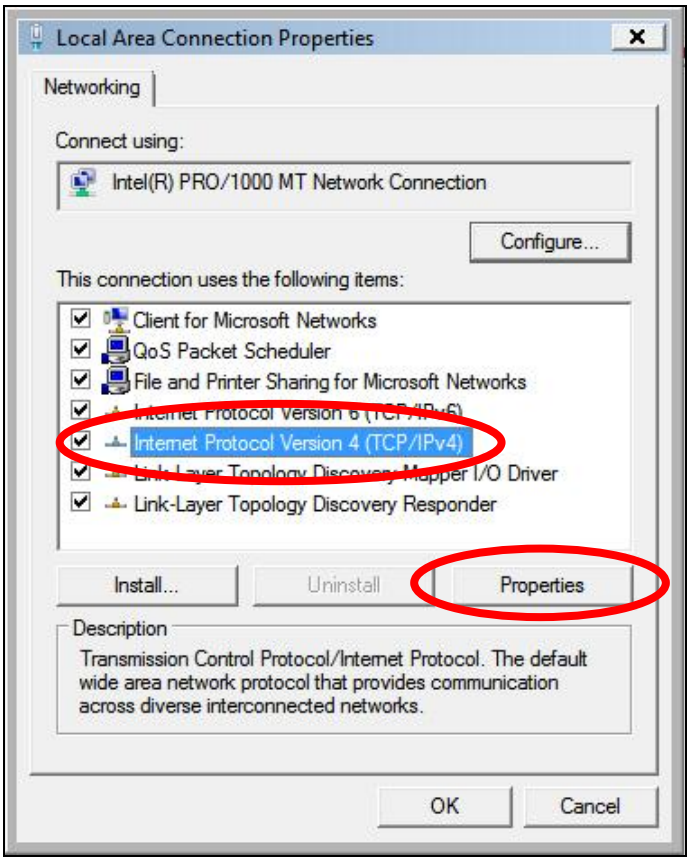
IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 2 . 10
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

IV-1-2-2. Windows Vista

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Click “View Network Status and Tasks”, then click “Manage Network Connections”. Right-click “Local Area Network”, then select “Properties”. The “Local Area Connection Properties” window will then appear, select “Internet Protocol Version 4 (TCP / IPv4)”, and then click “Properties”.

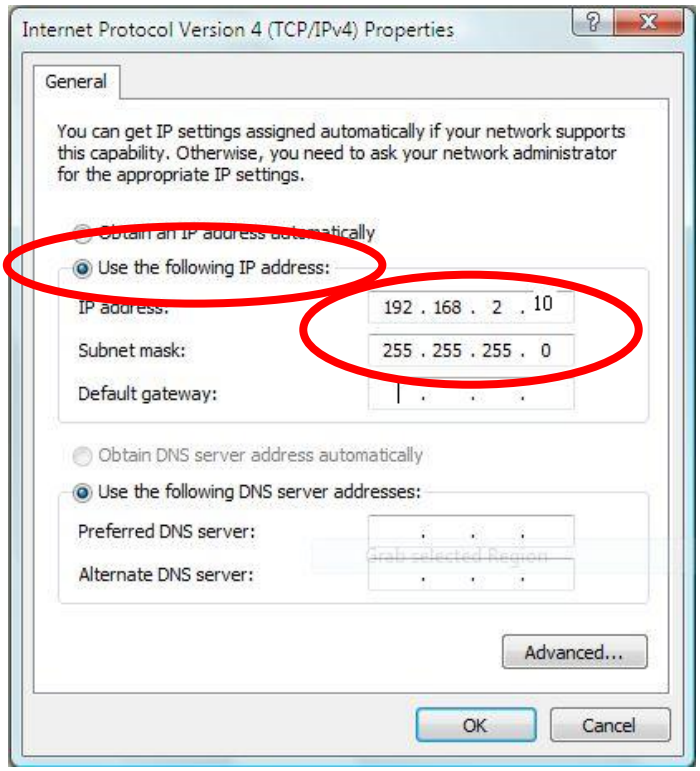


2. Select “Use the following IP address”, then input the following values:

Your existing static IP address will be displayed in the “IP address” field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

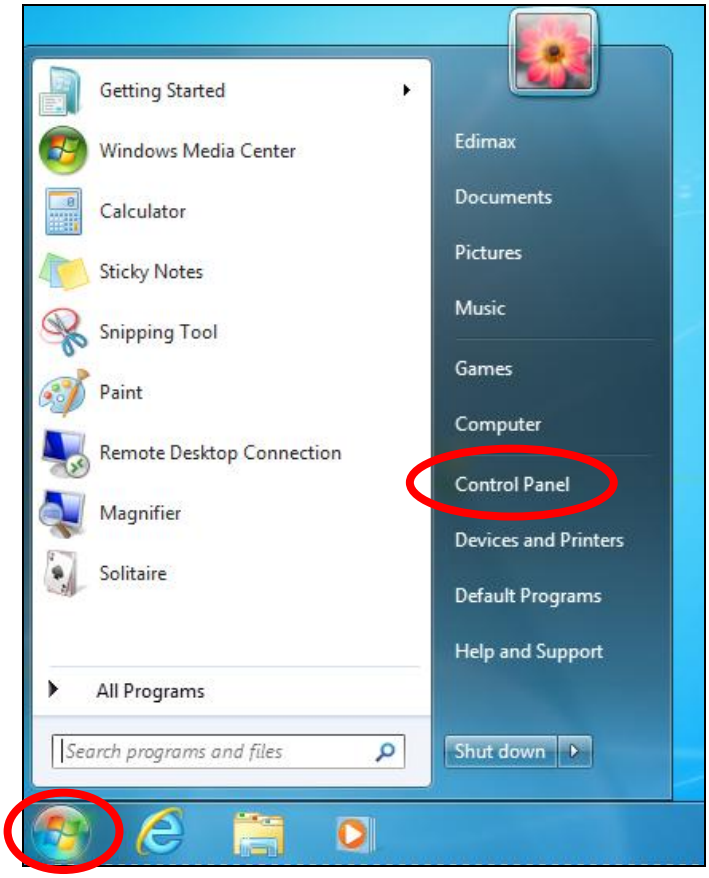
IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

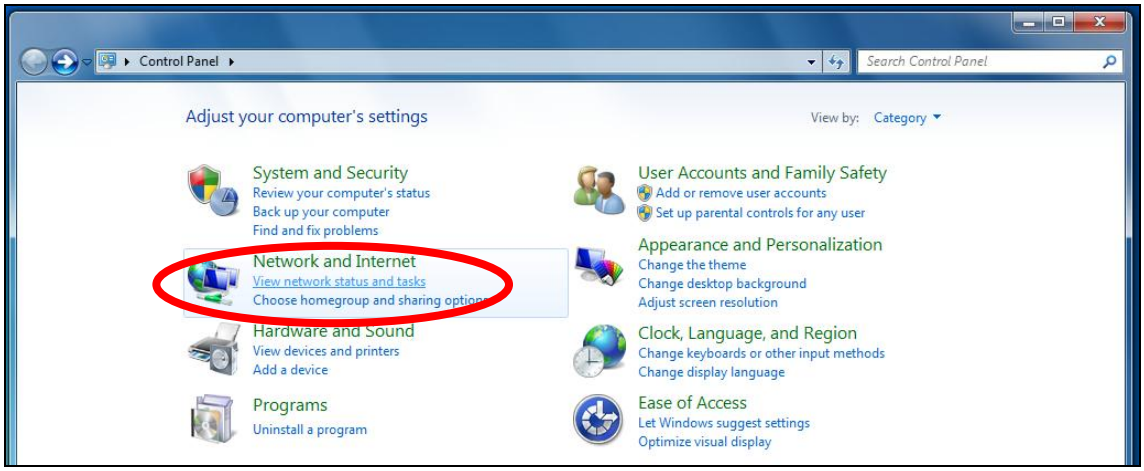

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Use the following IP address:
IP address:
192 . 168 . 2 . 10
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

IV-1-2-3. Windows 7

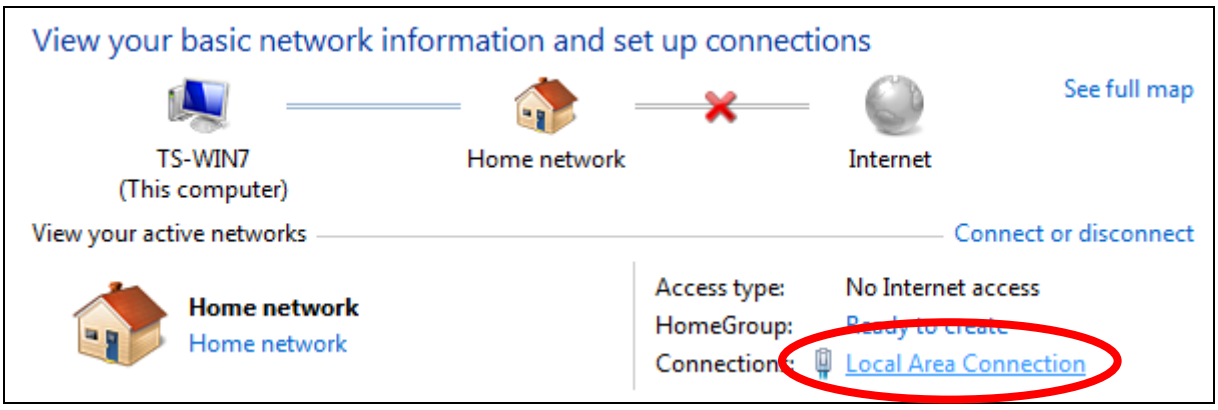
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



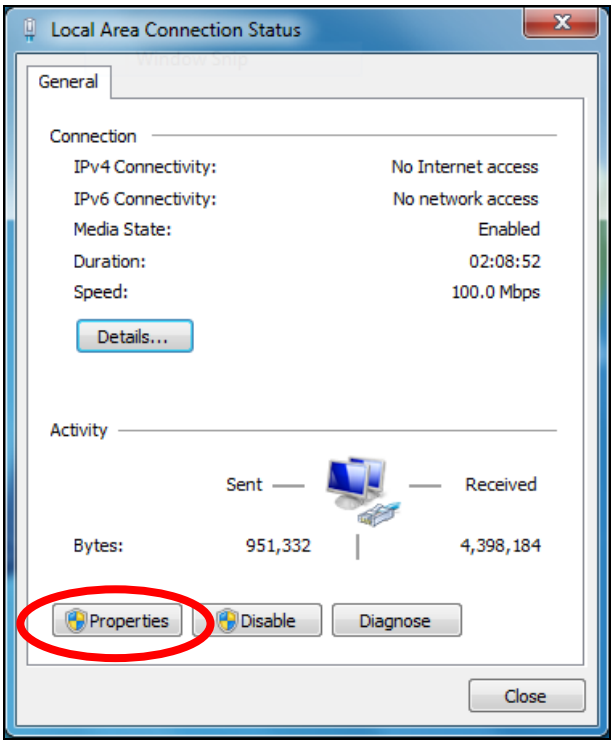
2. Under “Network and Internet” click “View network status and tasks”.



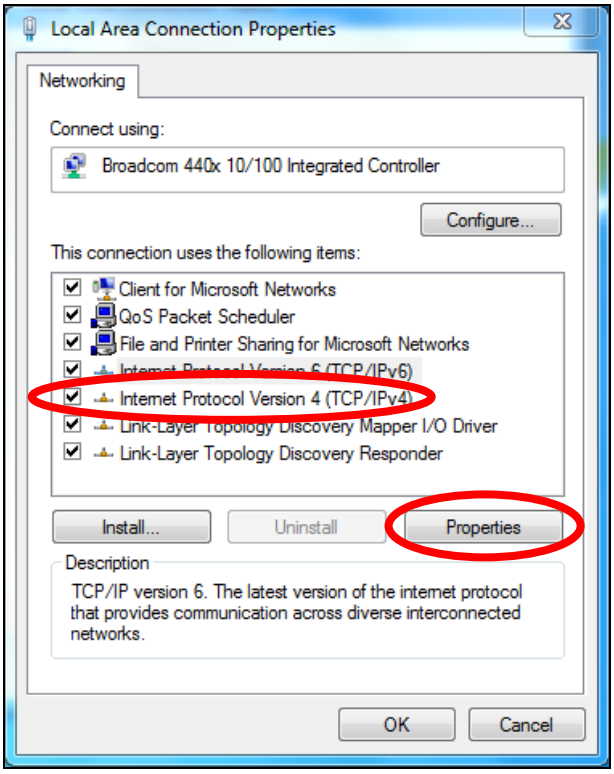
3. Click “Local Area Connection”.



4. Click “Properties”.



5. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.

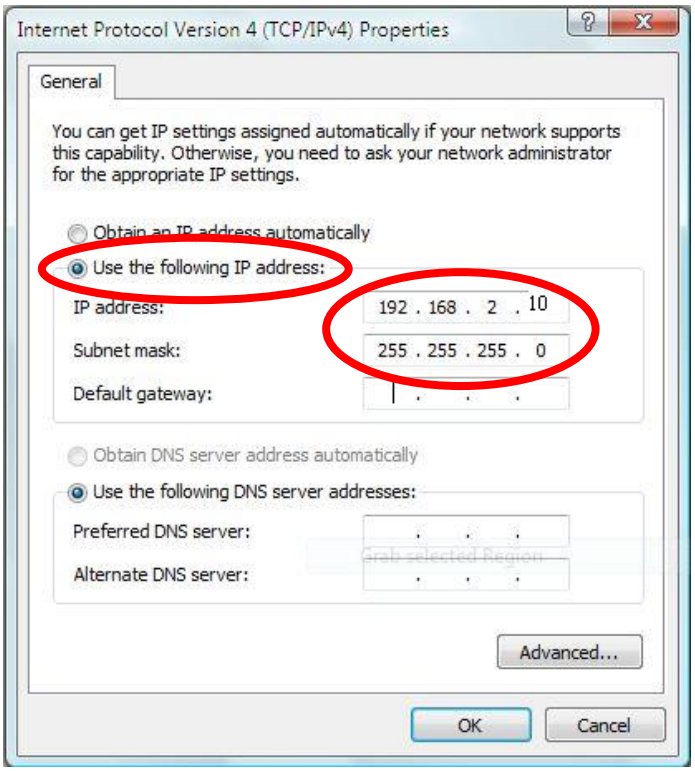


6. Select “Use the following IP address”, then input the following values:

Your existing static IP address will be displayed in the “IP address” field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

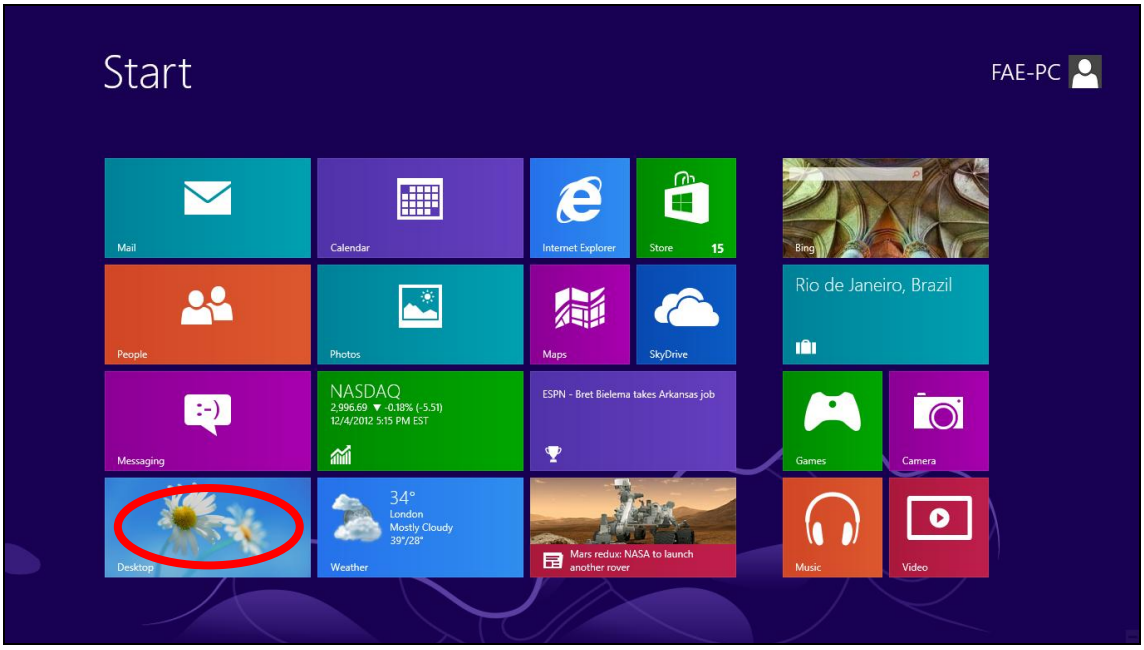
IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

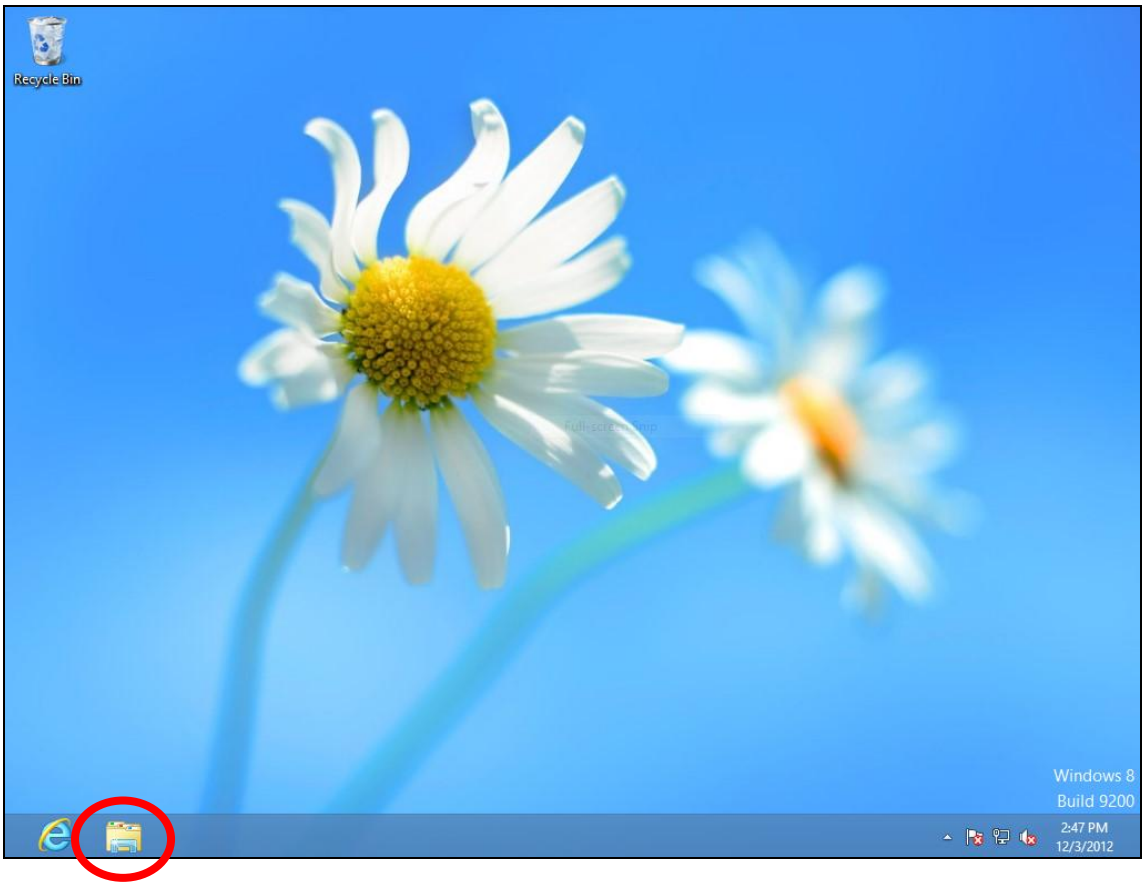

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 2 . 10
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

IV-1-2-4. Windows 8

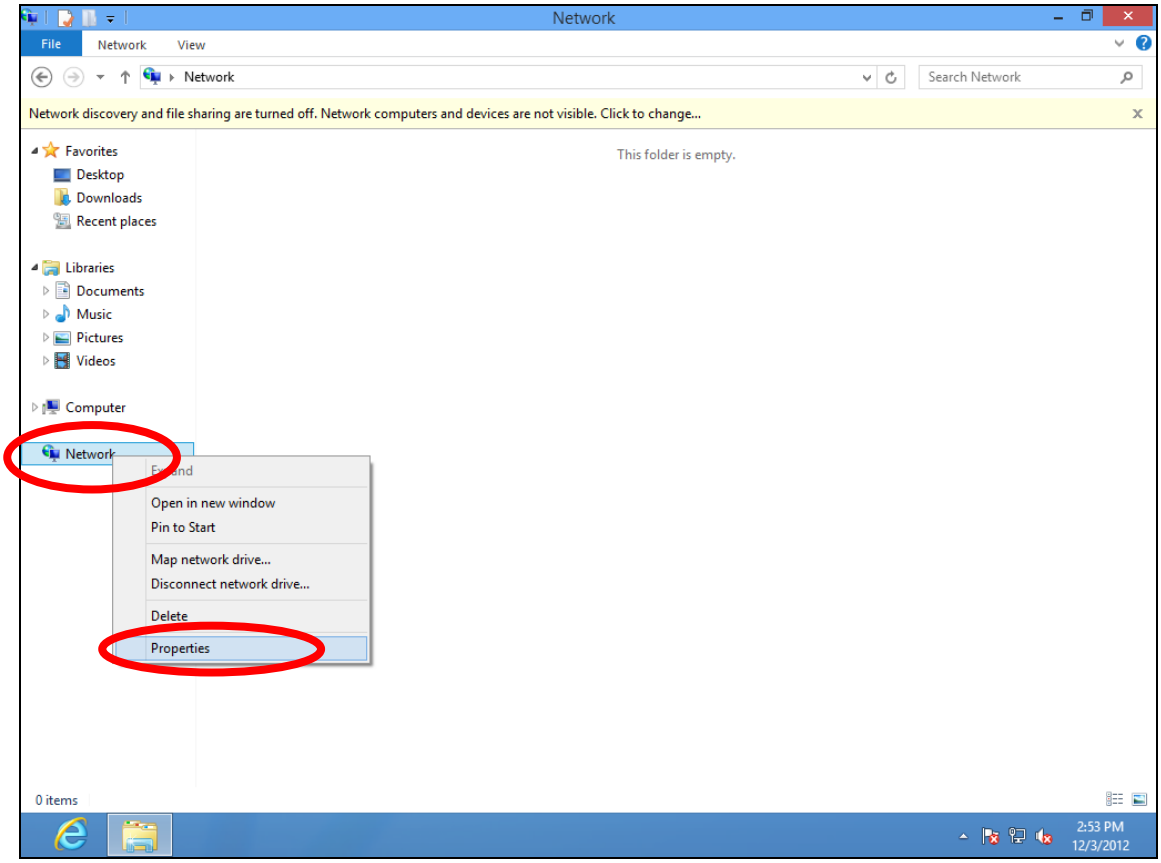
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your curser to the bottom left of the screen and click.



2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.

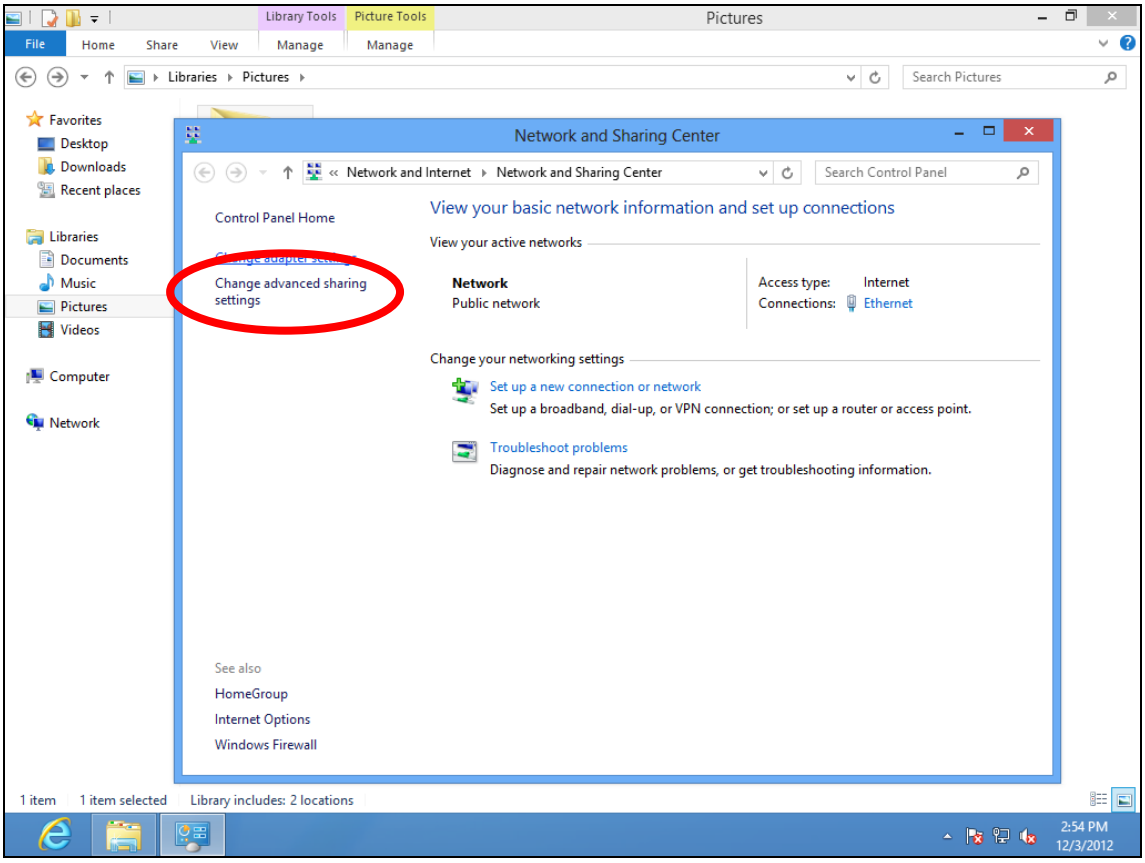


3. Right click “Network” and then select “Properties”.

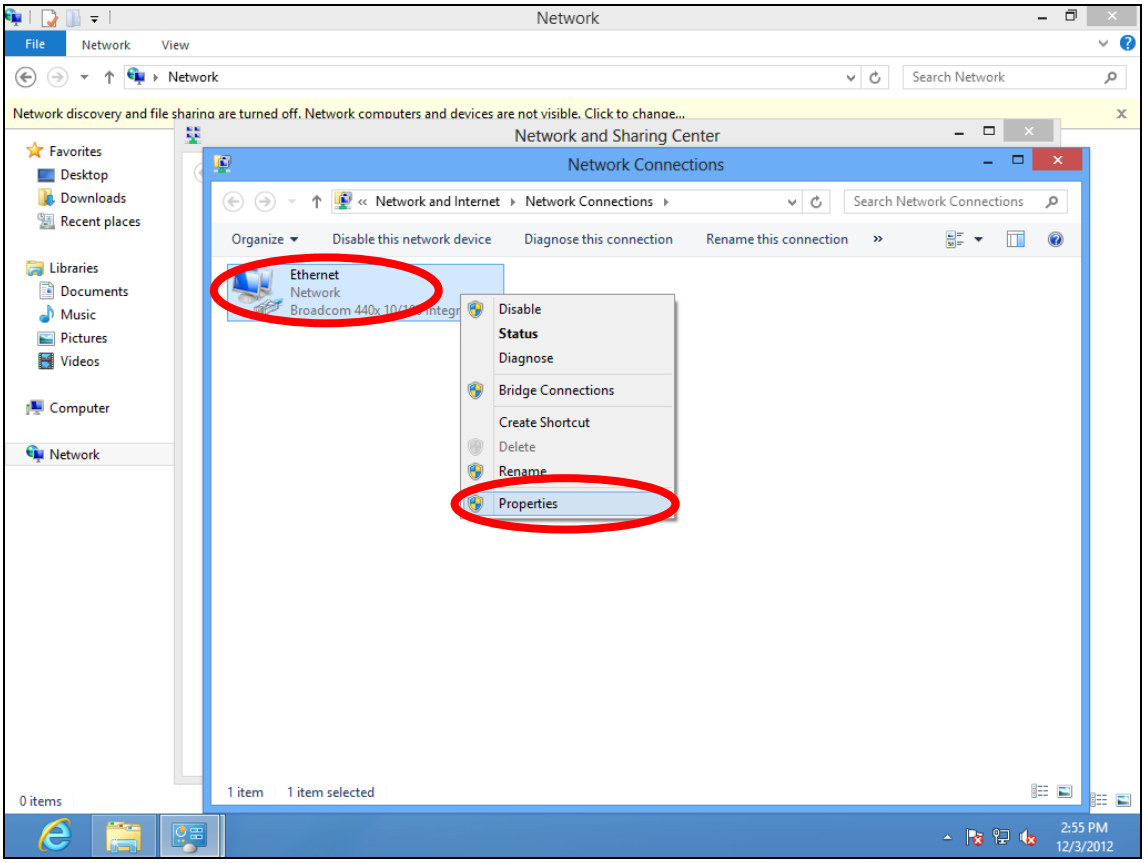


4. In the window that opens, select “Change adapter settings” from the left

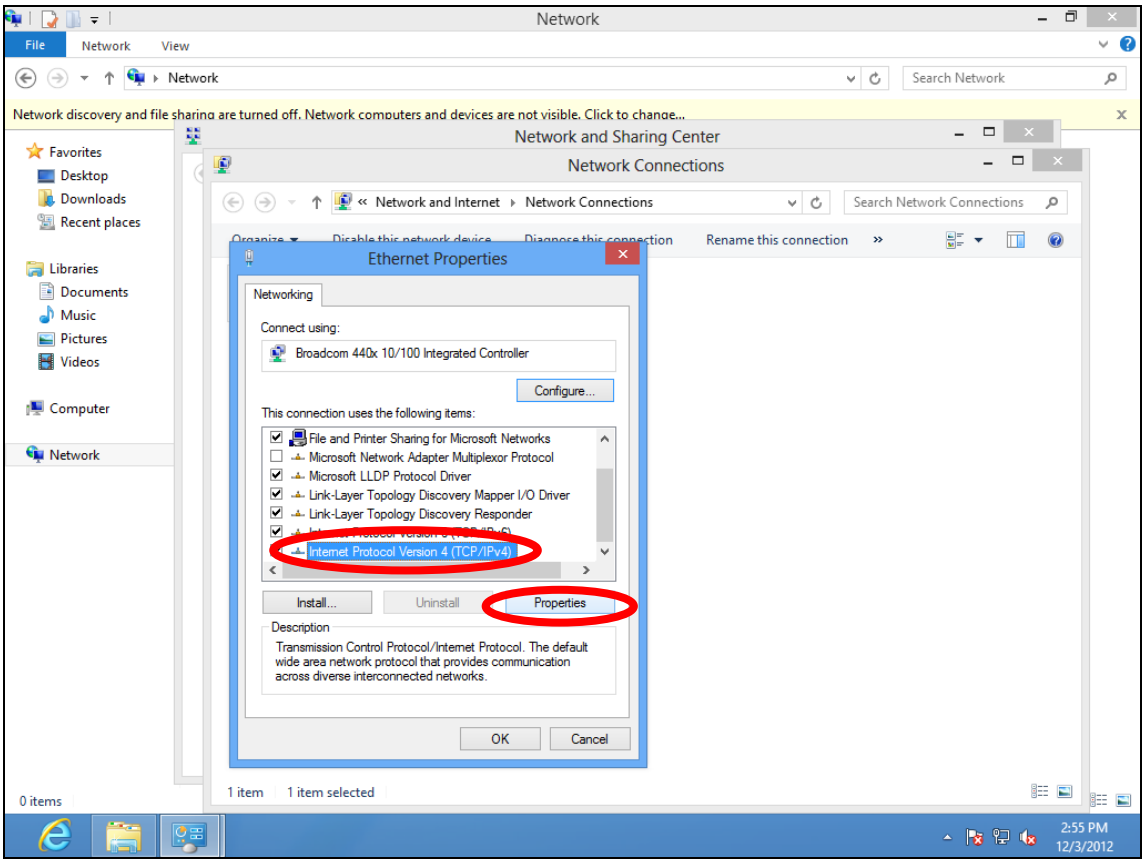
side.



5. Choose your connection and right click, then select “Properties”.



6. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.



7. Select “Use the following IP address”, then input the following values:

Your existing static IP address will be displayed in the “IP address” field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

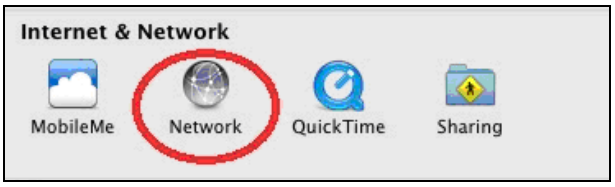
IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

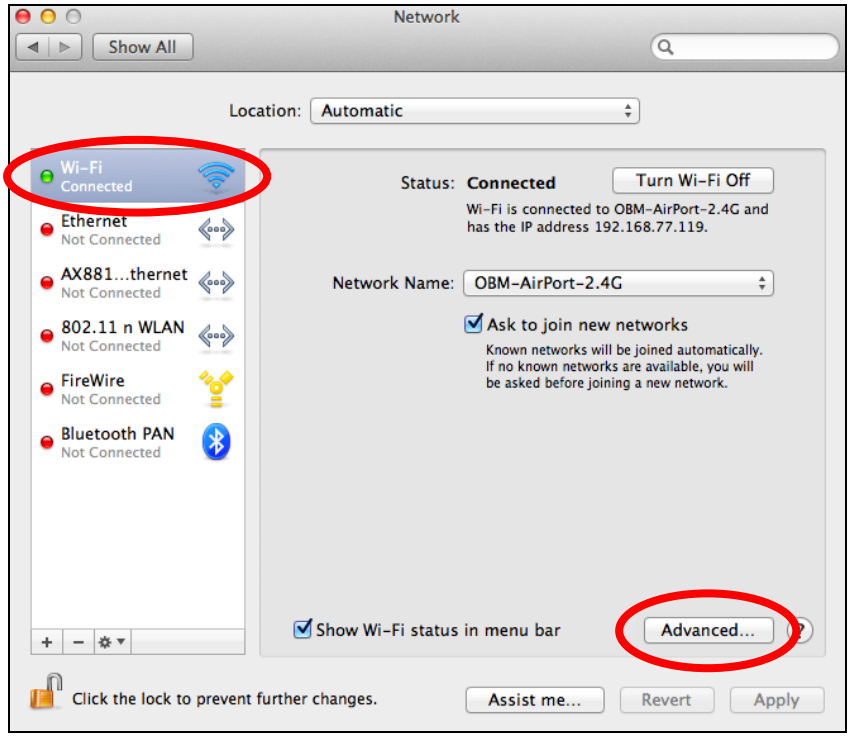
IV-1-2-5. Mac

1. Have your Macintosh computer operate as usual, and click on “System Preferences”

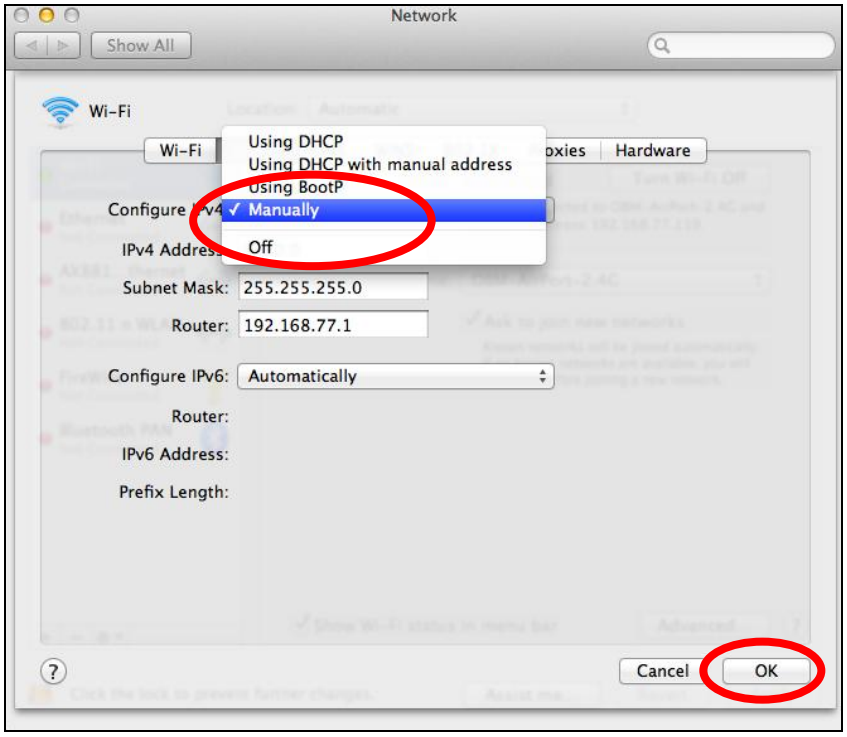
2. In System Preferences, click on “Network”.



3. Click on “Wi-Fi” in the left panel and then click “Advanced” in the lower right corner.

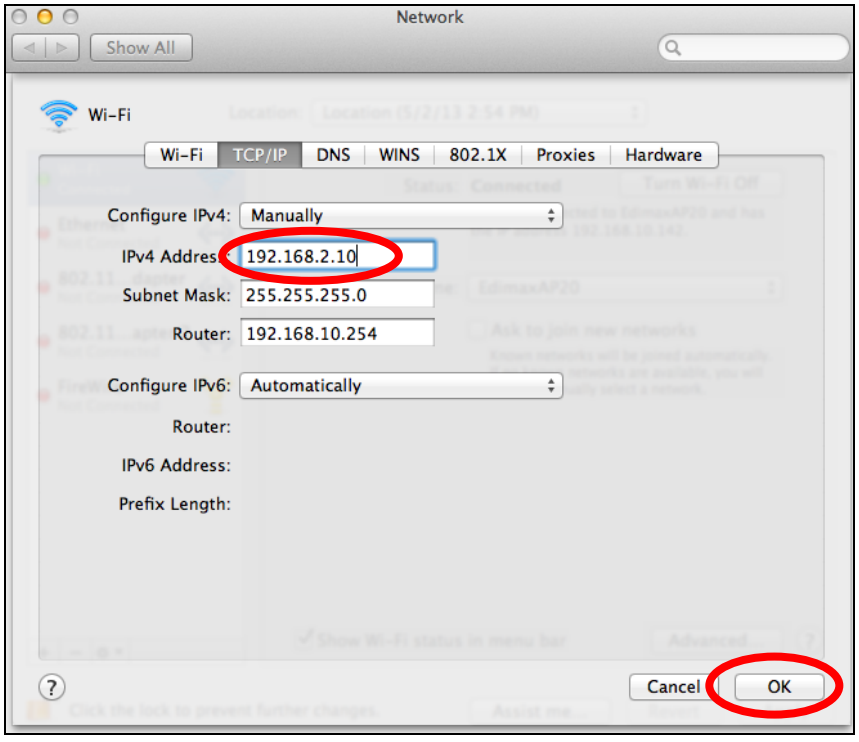


4. Select “TCP/IP” from the top menu and select “Manually” from the drop down menu labeled “Configure IPv4”, then click “OK”.

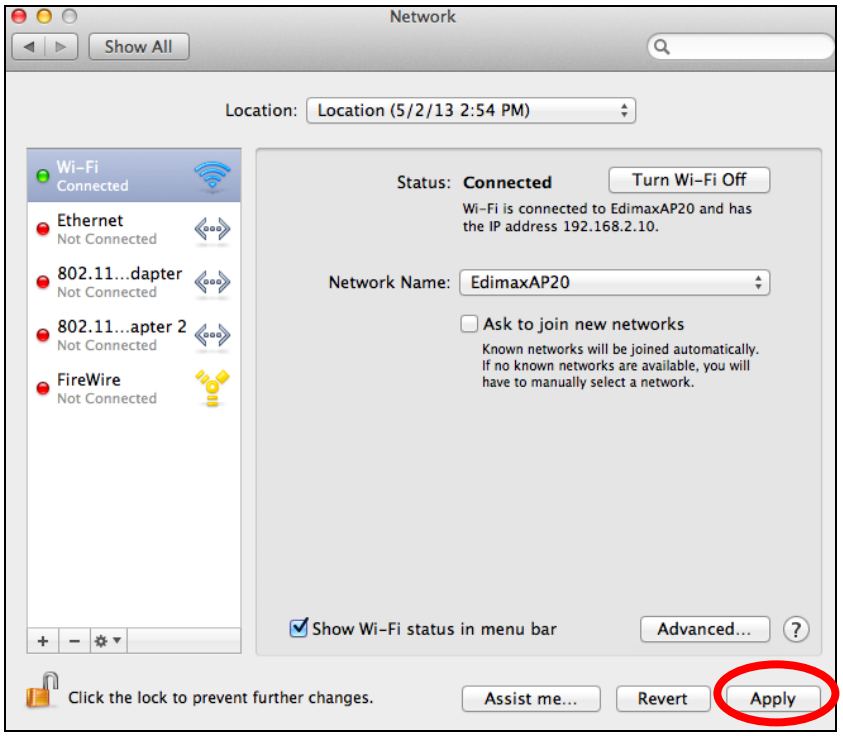


Your existing static IP address will be displayed in the "IP address" field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

5. In the "IPv4 Address" and "Subnet Mask" field enter IP address 192.168.2.10 and subnet mask 255.255.255.0. Click on "OK".



6. Click “Apply” to save the changes.



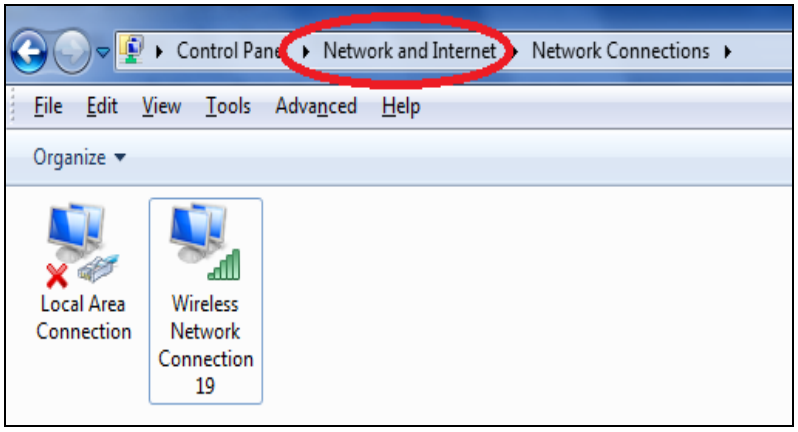
IV-1-3. How to Find Your Network Security Key

To find your network security key, please follow the instructions appropriate for your operating system.

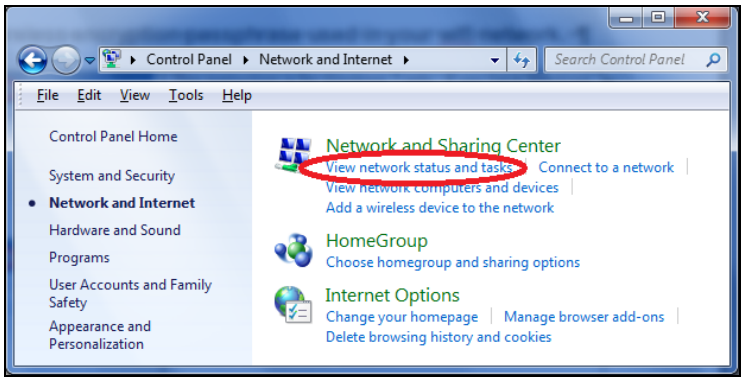
If you are using Windows XP or earlier, please contact your ISP or router manufacturer to find your network security key.

IV-1-3-1. Windows 7 & Vista

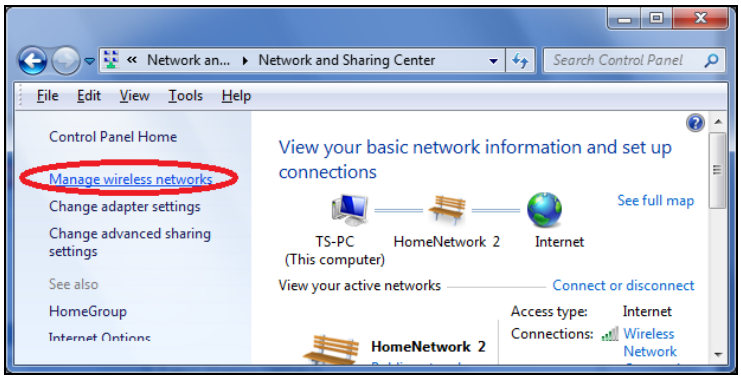
1. Open “Control Panel” and click on “Network and Internet” in the top menu.



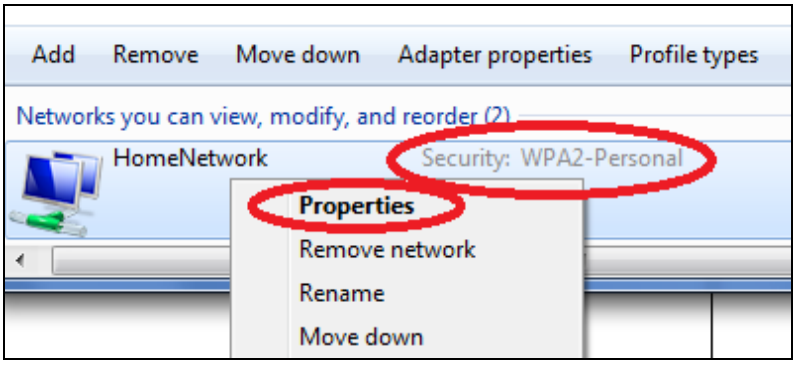
2. Click on “View network status and tasks” which is under the heading “Network and Sharing Center”.



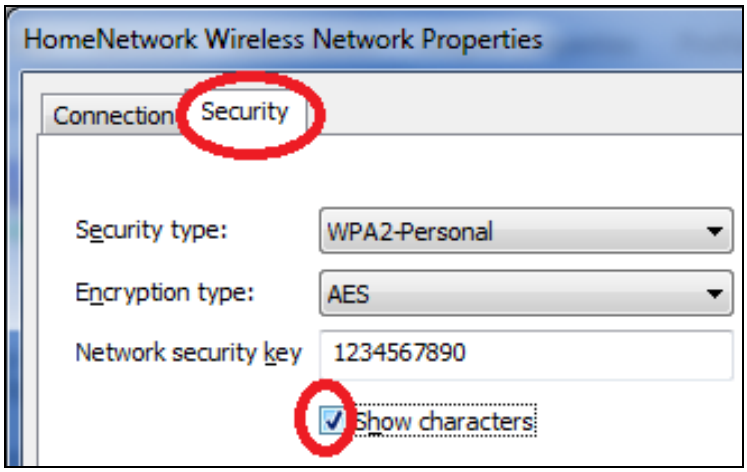
3. Click on “Manage wireless networks” in the left menu.



4. You should see the profile of your Wi-Fi network in the list. Right click on your Wi-Fi network and then click on “Properties”.

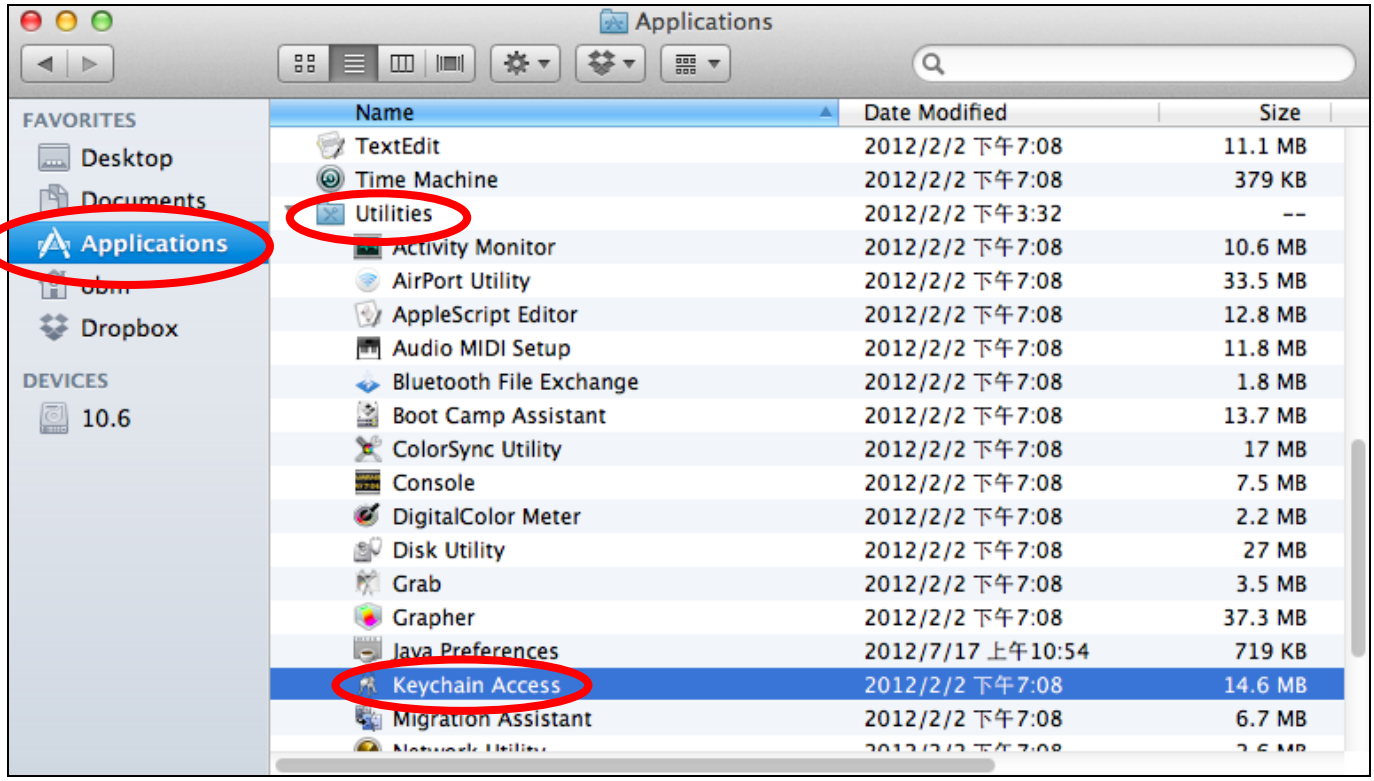


5. Click on the “Security” tab, and then check the box labeled “Show characters”. This will show your network security key. Click the “Cancel” button to close the window.

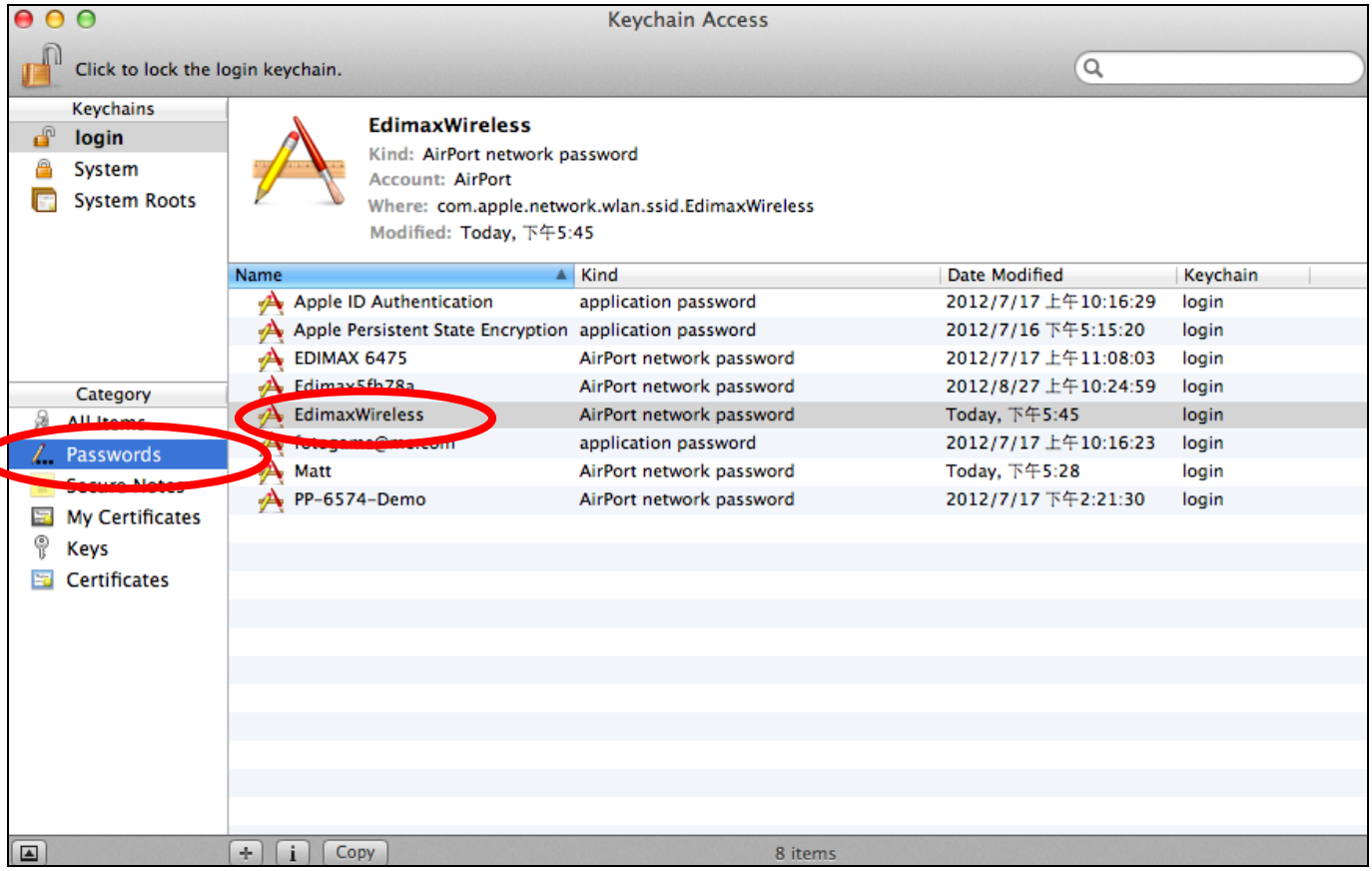


IV-1-3-2. Mac

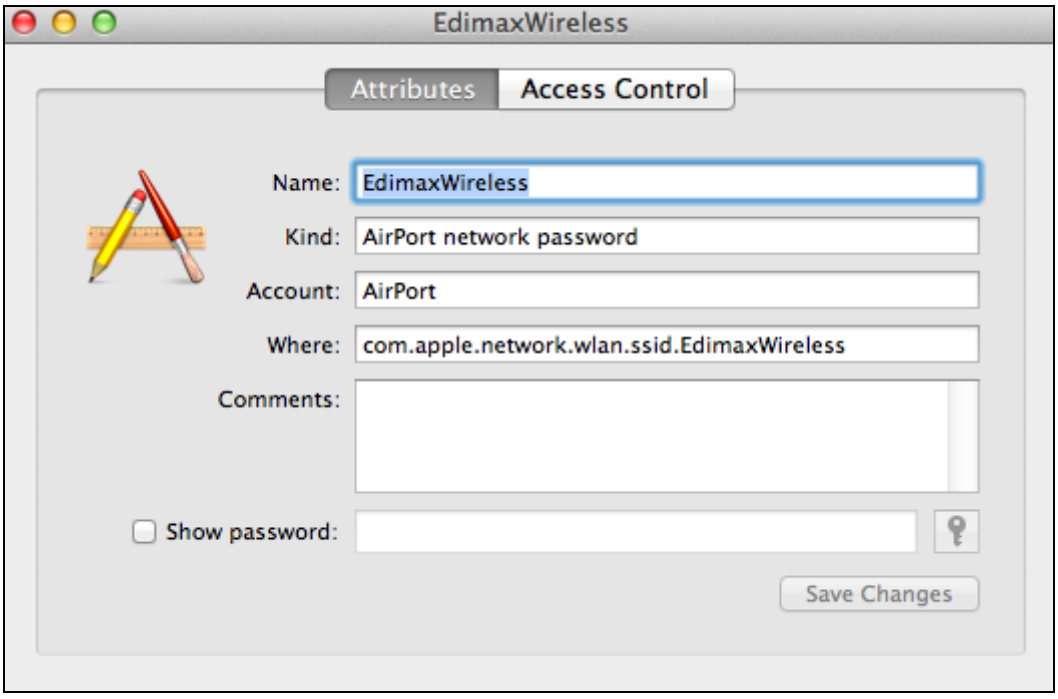
1. Open a new Finder window, and select “Applications” from the menu on the left side. Open the folder labeled “Utilities” and then open the application “Keychain Access”.


Applications
FAVORITES
Desktop
Documents
Applications
Dropbox
DEVICES
10.6
Name
Date Modified
Size
TextEdit 2012/2/2 下午7:08 11.1 MB
Time Machine 2012/2/2 下午7:08 379 KB
Utilities 2012/2/2 下午3:32 --
Activity Monitor 2012/2/2 下午7:08 10.6 MB
AirPort Utility 2012/2/2 下午7:08 33.5 MB
AppleScript Editor 2012/2/2 下午7:08 12.8 MB
Audio MIDI Setup 2012/2/2 下午7:08 11.8 MB
Bluetooth File Exchange 2012/2/2 下午7:08 1.8 MB
Boot Camp Assistant 2012/2/2 下午7:08 13.7 MB
ColorSync Utility 2012/2/2 下午7:08 17 MB
Console 2012/2/2 下午7:08 7.5 MB
DigitalColor Meter 2012/2/2 下午7:08 2.2 MB
Disk Utility 2012/2/2 下午7:08 27 MB
Grab 2012/2/2 下午7:08 3.5 MB
Grapher 2012/2/2 下午7:08 37.3 MB
Java Preferences 2012/7/17 上午10:54 719 KB
Keychain Access 2012/2/2 下午7:08 14.6 MB
Migration Assistant 2012/2/2 下午7:08 6.7 MB

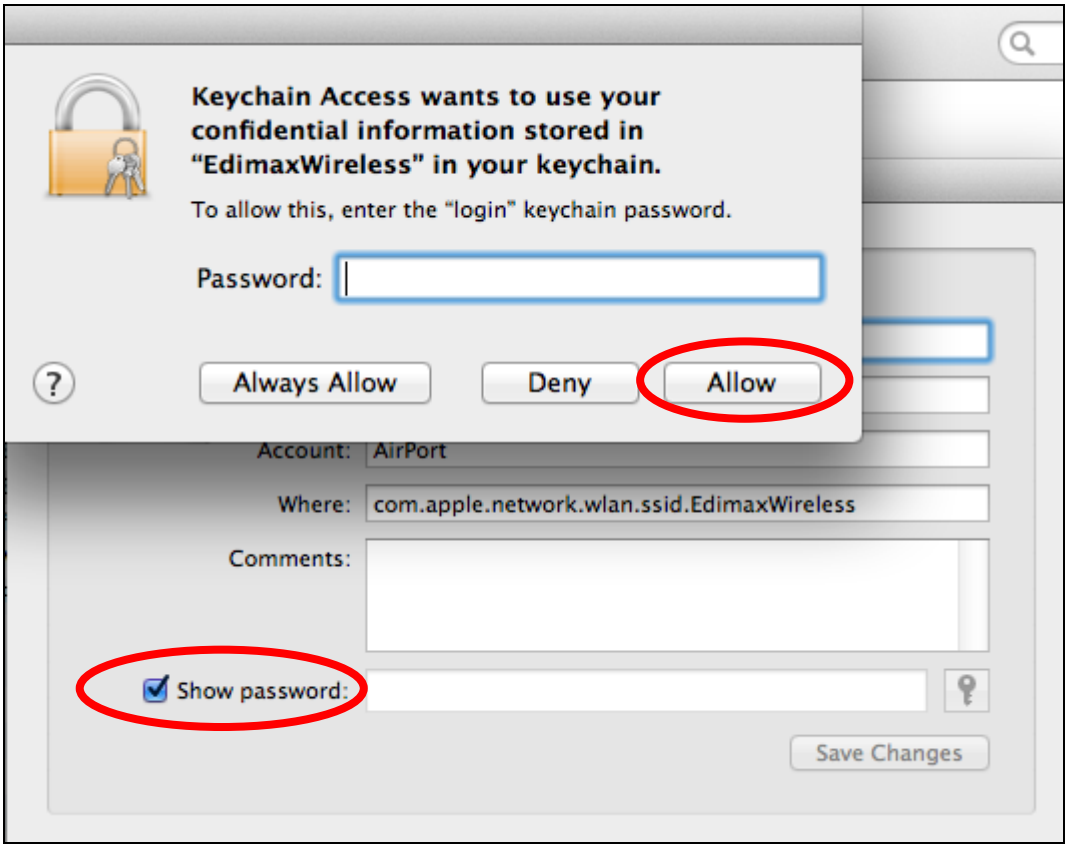
2. Select “Passwords” from the sub-menu labeled “Category” on the left side, as shown below. Then search the list in the main panel for the SSID of your network. In this example, the SSID is “EdimaxWireless” – though your SSID will be unique to your network.



3. Double click the SSID of your network and you will see the following window.



4. Check the box labeled “Show password” and you will be asked to enter your administrative password, which you use to log into your Mac. Enter your password and click “Allow”.



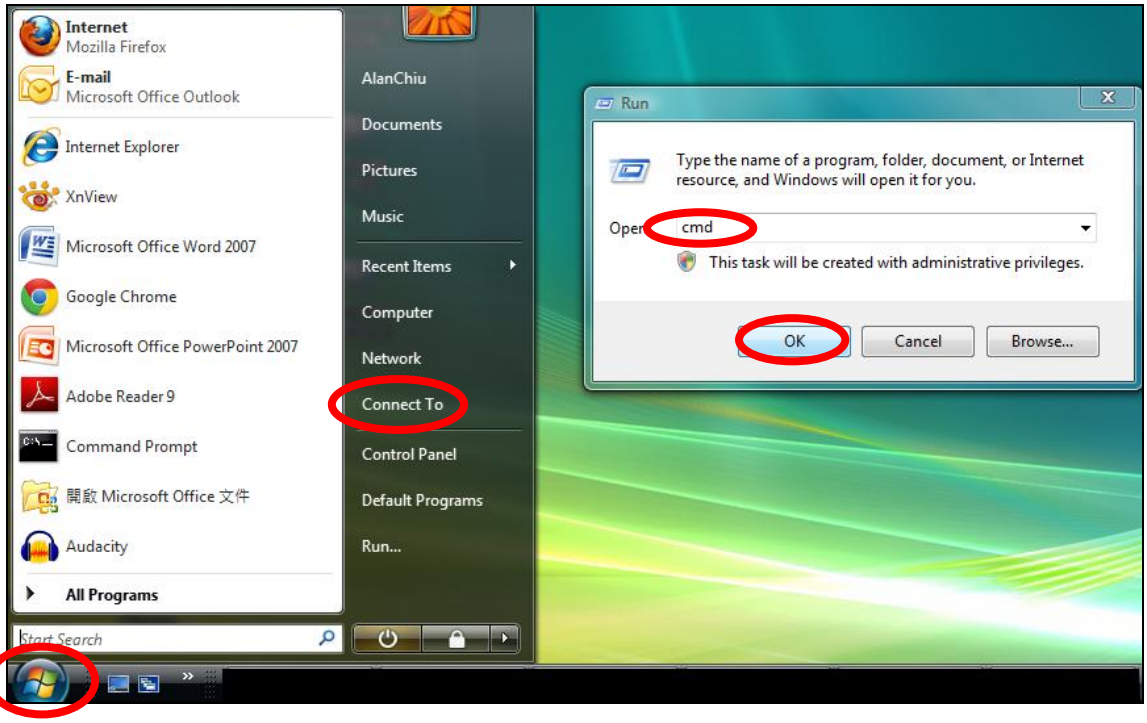
Your network security password will now be displayed in the field next to the box labeled “Show password”. In the example below, the network security password is “edimax1234”. Please make a note of your network security password.

IV-1-4. How to Find Your Router's IP Address

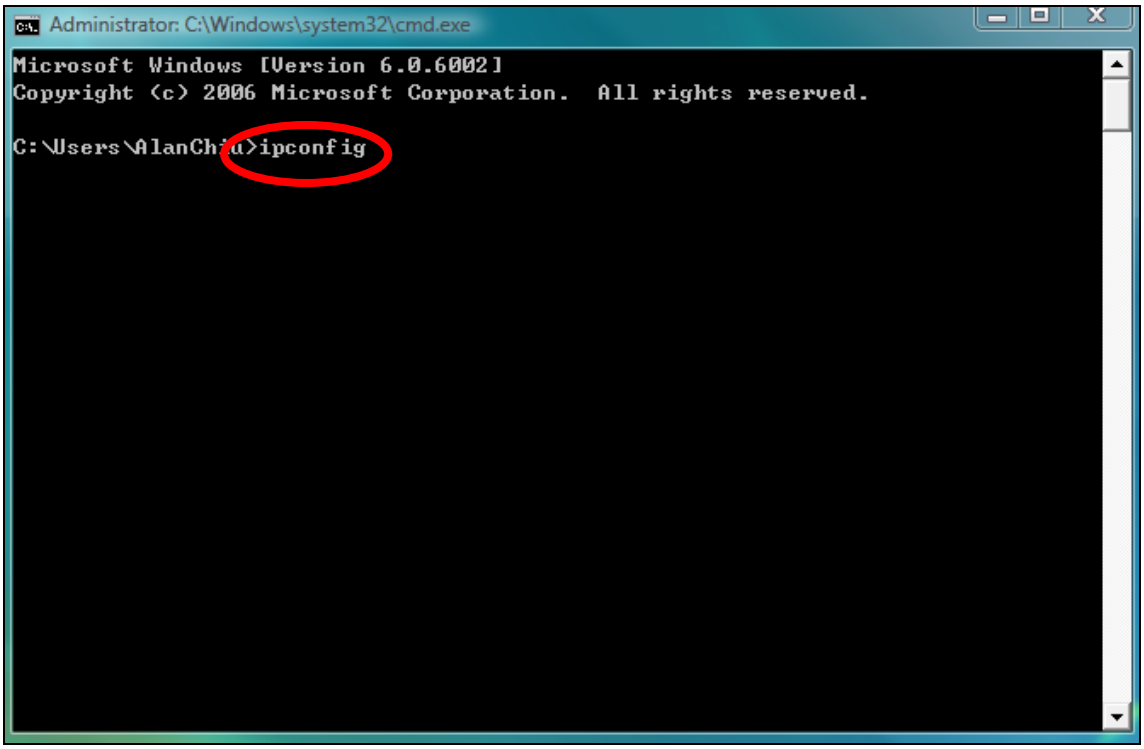
To find your router's IP address, please follow the instructions appropriate for your operating system.

IV-1-4-1. Windows XP, Vista & 7

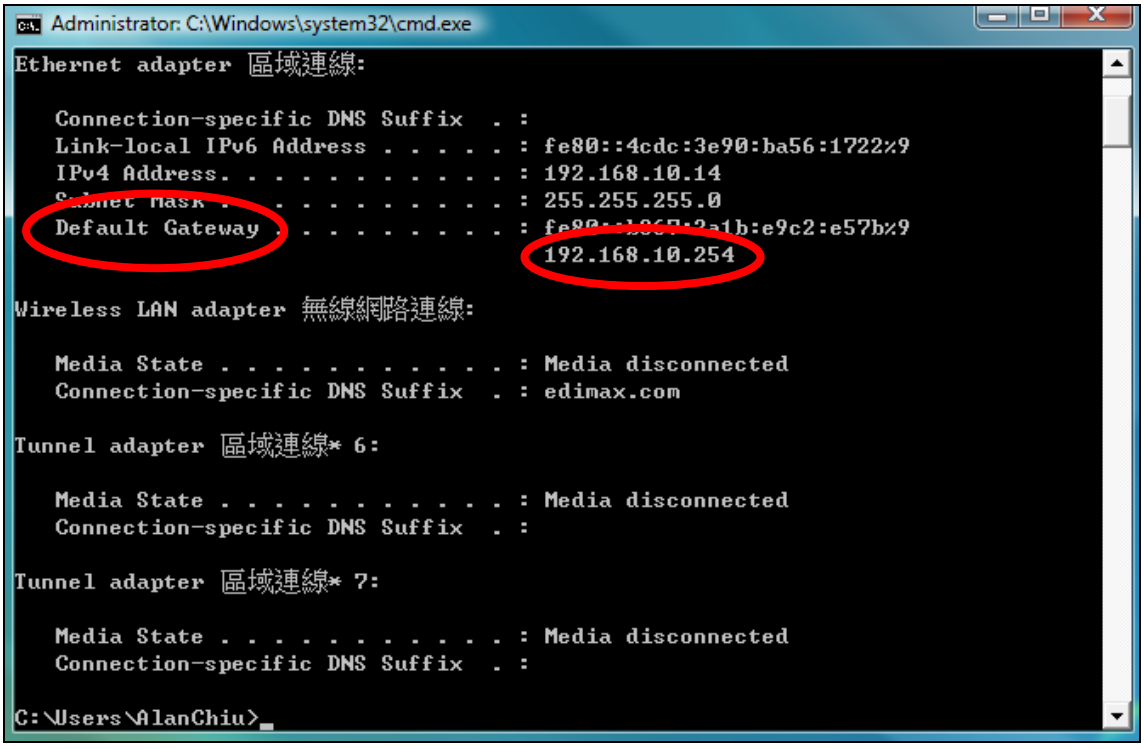
1. Go to "Start", select "Run" and type "cmd", then press Enter or click "OK".



2. A new window will open, type "ipconfig" and press Enter.



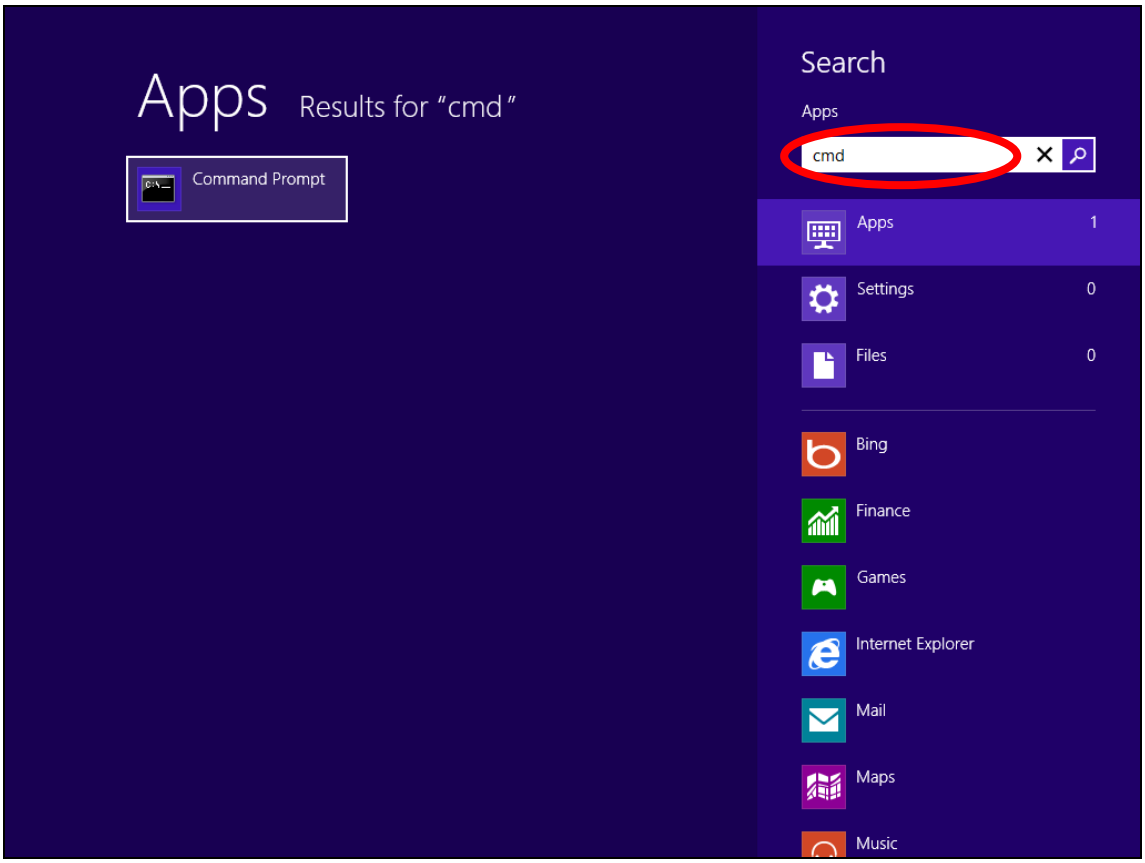
3. Your router's IP address will be displayed next to "Default Gateway".


Administrator: C:\Windows\system32\cmd.exe
Ethernet adapter 區域連線:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::4cdc:3e90:ba56:1722%9
IPv4 Address. . . . . : 192.168.10.14
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1867:3a1b:e9c2:e57b%9
192.168.10.254
Wireless LAN adapter 無線網路連線:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : edimax.com
Tunnel adapter 區域連線* 6:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter 區域連線* 7:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\AlanChiu>

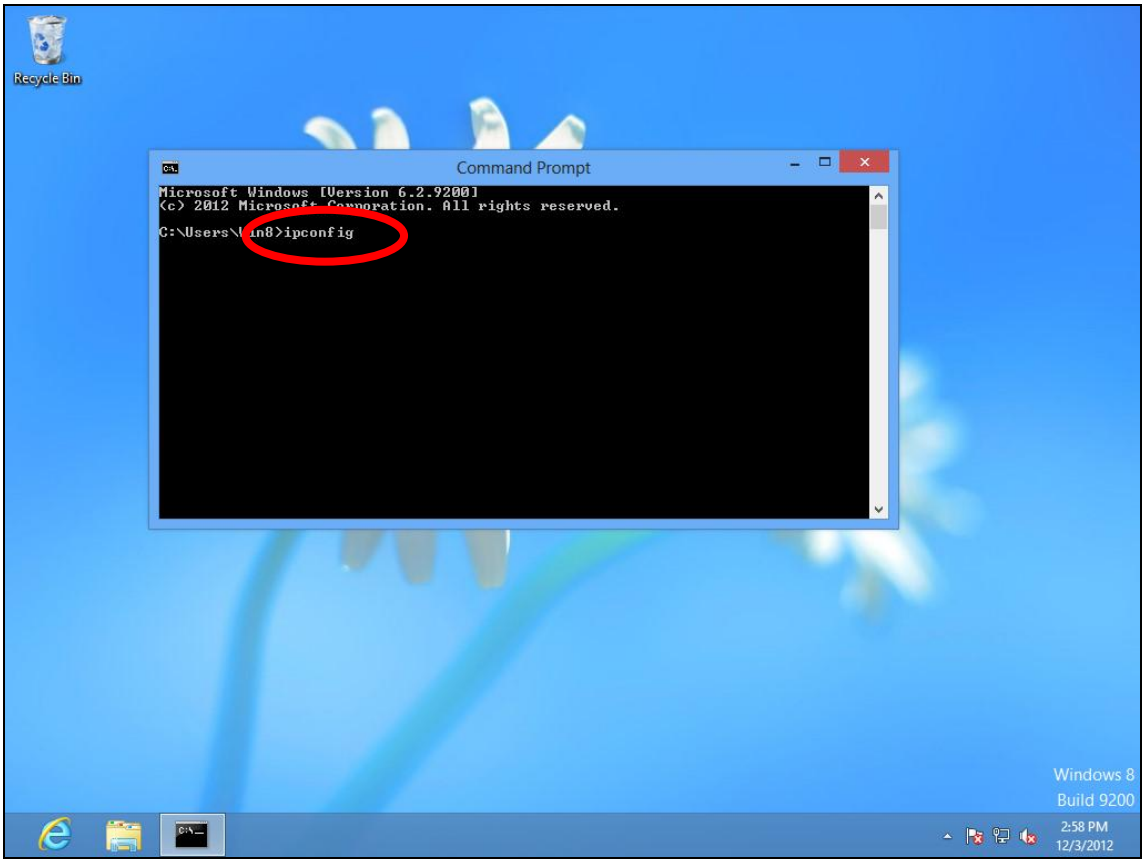
IV-1-4-2. Windows 8

1. From the Windows 8 Start screen, move your curser to the top right corner of the screen to display the Charms bar.

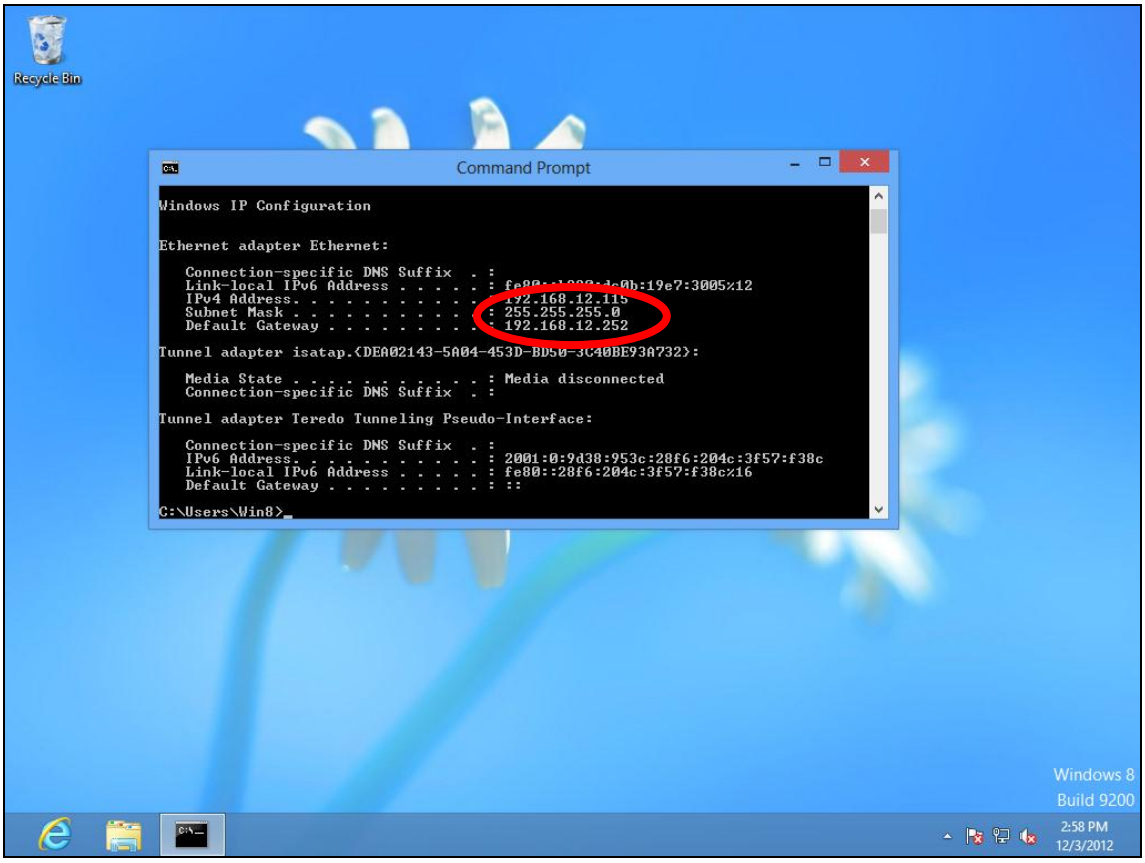
2. Click “Search” and enter “cmd” into the search bar. Click the “Command Prompt” app which be displayed on the left side.



3. A new window will open, type “ipconfig” and press Enter.



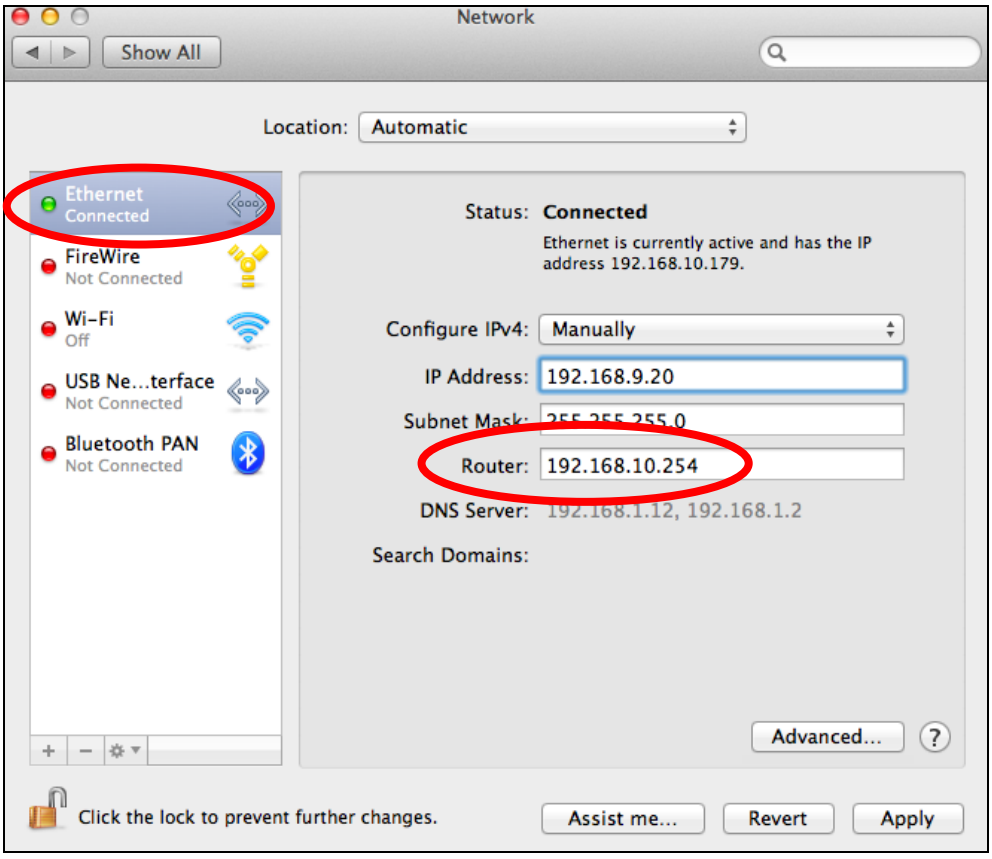
4. Your router's IP address will be displayed next to "Default Gateway".


Recycle Bin
Command Prompt
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::1888:dc0b:19e7:3005%12
IPv4 Address. . . . . : 192.168.12.115
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.12.252
Tunnel adapter isatap.{DEA02143-5A04-453D-BD50-3C40BE93A732}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:0:9d38:953c:28f6:204c:3f57:f38c
Link-local IPv6 Address . . . . . : fe80::28f6:204c:3f57:f38c%16
Default Gateway . . . . . : ::
C:\Users\Win8>
Windows 8
Build 9200
2:58 PM
12/3/2012

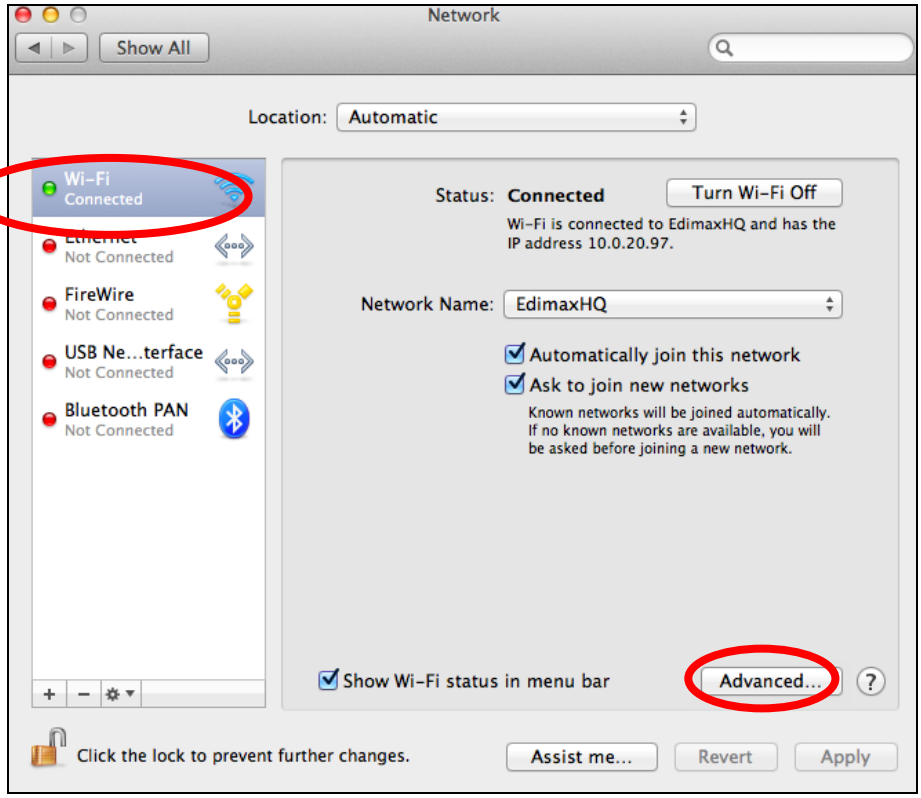
IV-1-4-3. Mac

1. Launch “System Preferences” and click on “Network”.

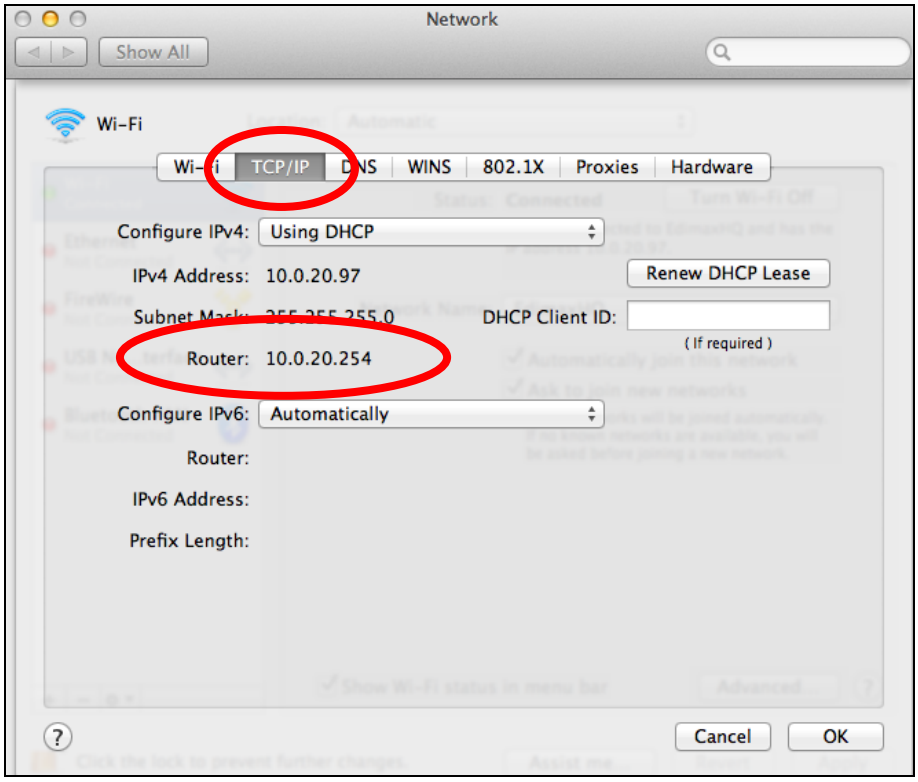
2. If you are using an Ethernet cable to connect to your network, your router’s IP address will be displayed next to “Router”.



3. If you are using Wi-Fi, click “Wi-Fi” in the left panel, and then “Advanced” in the bottom right corner.

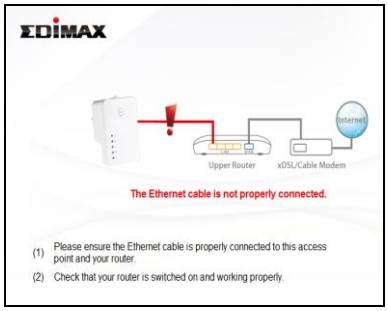


4. Click the "TCP/IP" tab and your router's IP address will be displayed next to "Router".



IV-1-4. Troubleshooting

If you are experiencing problems with your access point, please refer to the troubleshooting guide below before contacting your dealer of purchase for help.

Scenario	Solution
My Internet isn't working, or when I go to htto://EdimaxAP I see an error screen:**  EDIMAX Internet Upper Router xDSL/Cable Modem The Ethernet cable is not properly connected. (1) Please ensure the Ethernet cable is properly connected to this access point and your router. (2) Check that your router is switched on and working properly.	***1.*** *Ensure that your Ethernet cable is properly connected to the access point.* ***2.*** *Make sure that the access point is correctly plugged in and switched on.* **3.** *Check that your existing router is switched on and working properly.*
I can't access the URL http://EdimaxAP, but my Internet is working.**	***1.*** *Ensure you include "**http://**" in the URL.* ***2.*** *Reconnect to the access point's SSID "EdimaxAP**" and try again.* ***3.*** *For first time access, your wireless device must use a dynamic IP address. Static IP users need to temporarily modify their IP address and go to the access point's default IP address **192.168.2.2** instead of the URL. Please refer to **IV-1. Configuring your IP address** for more information.*
Streaming on my wireless device is slow or frequently interrupted.	***1.*** *Reset the access point.* ***2.*** *Try again later. Your local network may be experiencing technical difficulties or very high usage.* **3.** *Change the channel number of your wireless network.*
I can't log onto the browser based configuration interface: incorrect password.	***1.*** *Password is case-sensitive. Make sure the "Caps Lock" light is not illuminated.* **2.** *If you do not know your password, restore the device to factory settings.*
The access point is	***1.*** *It is normal for the access point to heat up during*

extremely hot.	*frequent use. If you can safely place your hand on the access point, the temperature of the device is at a normal level.* **2.** *If you smell burning or see smoke coming from the access point or A/C power adapter, then disconnect the access point and A/C power adapter immediately as far as it is safely possible to do so. Call your dealer of purchase for help.*
My network is using a static IP address, how do I assign an IP address to my access point?	***1.*** *You can modify the IP address of the access point using the browser based configuration interface. Please refer to* ***IV-1. Configuring your IP address*** *for more information, and* ***III-6. System Utility*** *to modify the access point's IP address.*

IV-1-5. Glossary

Default Gateway (Access point): Every non-access point IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandaccess point.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandaccess point.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.
When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000
It means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for access points to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet access point located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband access point's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.
Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

Access point: A access point is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).
TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

COPYRIGHT

Copyright © Edimax Technology Co., Ltd. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission from Edimax Technology Co., Ltd.

Edimax Technology Co., Ltd. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Any software described in this manual is sold or licensed as is. Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Edimax Technology Co., Ltd. reserves the right to revise this publication and to make changes from time to time in the contents hereof without the obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such as PDAs or lap pads is not authorized. This transmitter is restricted for use with the specific antenna tested in the application for certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 1999/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 1999/5/ES, 2009/125/ES, 2006/95/ES, 2011/65/ES.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (1999/5/EK, 2009/125/EK, 2006/95/EK, 2011/65/EK).

Türkçe: Bu cihaz 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 1999/5/ES, 2009/125/ES, 2006/95/ES, 2011/65/ES.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 1999/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..

Português: Este equipamento cumpre os requesitos essênciais da Directiva 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 1999/5/EG, 2009/125/EG, 2006/95/EG, 2011/65/EG.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

suomen kieli: Tämä laite täyttää direktiivien 1999/5/EY, 2009/125/EY, 2006/95/EY, 2011/65/EY oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN AT BE CY CZ DK EE FI FR DE GR HU IE IT LV LT LU MT NL PL PT SK SI ES SE GB IS LI NO CH BG RO TR

N20379

АЯ46

WEEE Directive & Product Disposal

At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European R&TTE directive 1999/5/EC, and 2009/125/EC, 2006/95/EC, 2011/65/EC .

Equipment: **N300 Wall-plug Access Point**
Model No.: **EW-7438APn**

The following European standards for essential requirements have been followed:

Spectrum: **ETSI EN 300 328 V1.7.1 (2006-10)**
EMC: **EN 301 489-1 V1.9.2 (2011-09);**
EN 301 489-17 V2.1.1 (2009-05)
EMF: **EN 50385:2002**
Safety (LVD): **IEC 60950-1:2005 (2nd Edition);**
EN-60950-1:2006+A11:2009+A1:2010+A12:2011

Edimax Technology Co., Ltd.
No. 3, Wu Chuan 3rd Road,
Wu-Ku Industrial Park,
New Taipei City, Taiwan

CE

Date of Signature: November 15, 2011
Signature:

Printed Name: Albert Chang
Title: Director
Edimax Technology Co., Ltd.

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. „Free Software“, der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The ‘“Program’“, below, refers to any such program or work, and a ‘“work based on the Program’“ means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term ‘“modification’“.) Each licensee is addressed as ‘“you’“.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and '"any later version'", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM '"AS IS'" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

EDIMAX

NETWORKING PEOPLE TOGETHER

Edimax Technology Co., Ltd.
No.3, Wu-Chuan 3rd Road, Wu-Gu,
New Taipei City 24891, Taiwan

Edimax Technology Europe B.V.
Nijverheidsweg 25 5683 CJ Best
The Netherlands

Edimax Computer Company
3350 Scott Blvd., Bldg.15 Santa Clara,
CA 95054, USA